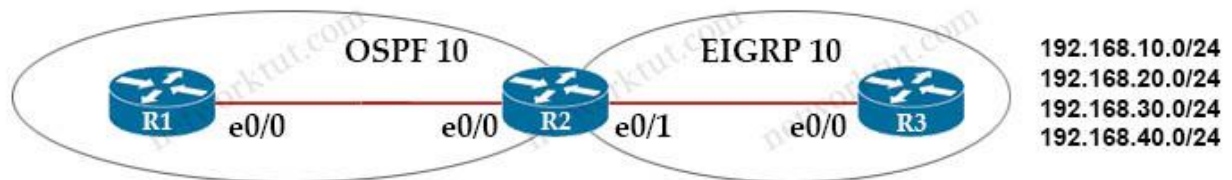


# New ENARSI Questions 5

## Question 1

Refer to the exhibit.



An engineer must redistribute networks 192.168.10.0/24 and 192.168.20.0/24 into OSPF from EIGRP, where the metric must be added when traversing through multiple hops to start an external route of 20. The engineer notices that the external metric is fixed and does not add at each hop. Which configuration resolves the issue?

<p>Option A</p> <pre>R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255 R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255 ! R2(config)#route-map RD permit 10 R2(config-route-map)#match ip address 10 R2(config-route-map)#set metric 20 R2(config-route-map)#set metric-type type-2 ! R2(config)#router ospf 10 R2(config-router)#redistribute eigrp 10 subnets route-map RD</pre>	<p>Option B</p> <pre>R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255 R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255 ! R2(config)#route-map RD permit 10 R2(config-route-map)#match ip address 10 R2(config-route-map)#set metric 20 R2(config-route-map)#set metric-type type-1 ! R2(config)#router ospf 10 R2(config-router)#redistribute eigrp 10 subnets route-map RD</pre>
<p>Option C</p> <pre>R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255 R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255 ! R1(config)#route-map RD permit 10 R1(config-route-map)#match ip address 10 R1(config-route-map)#set metric 20 R1(config-route-map)#set metric-type type-1 ! R1(config)#router ospf 10 R1(config-router)#redistribute eigrp 10 subnets route-map RD</pre>	<p>Option D</p> <pre>R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255 R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255 ! R1(config)#route-map RD permit 10 R1(config-route-map)#match ip address 10 R1(config-route-map)#set metric 20 R1(config-route-map)#set metric-type type-2 ! R1(config)#router ospf 10 R1(config-router)#redistribute eigrp 10 subnets route-map RD</pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

### Question 2

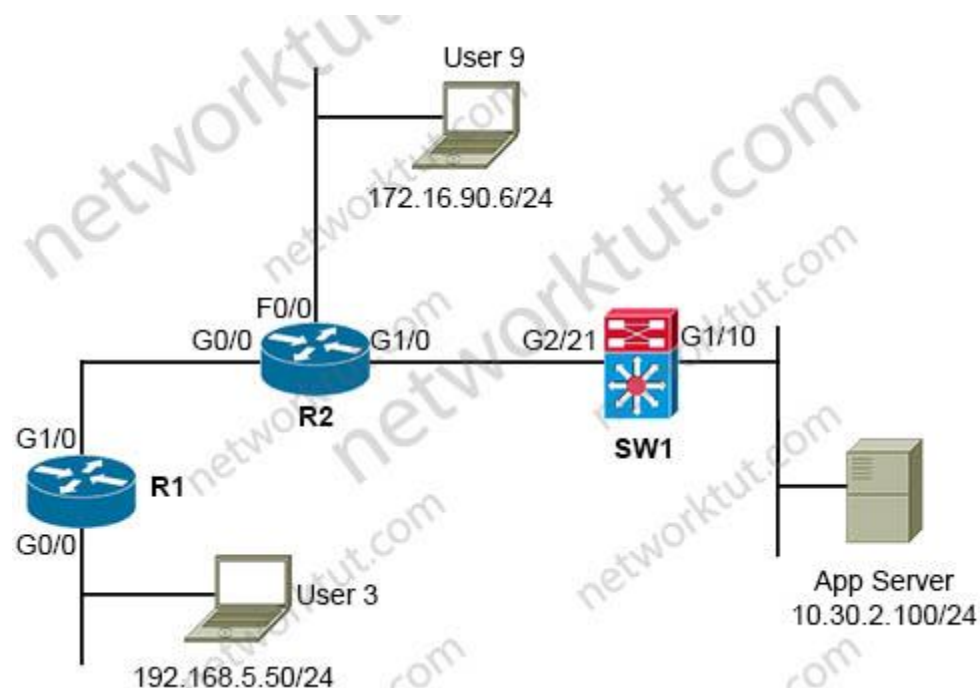
An engineer notices that R1 does not hold enough log messages to identify the root cause during troubleshooting. Which command resolves this issue?

- A. #logging buffered 4096 critical
- B. #logging buffered 16000 critical
- C. (config)#logging buffered 16000 informational
- D. (config)#logging buffered 4096 informational

**Answer: C**

### Question 3

Refer to the exhibit.



A network administrator must block **ping** from user 3 to the App Server only. An inbound standard access list is applied to R1 interface G0/0 to block **ping**. The network administrator

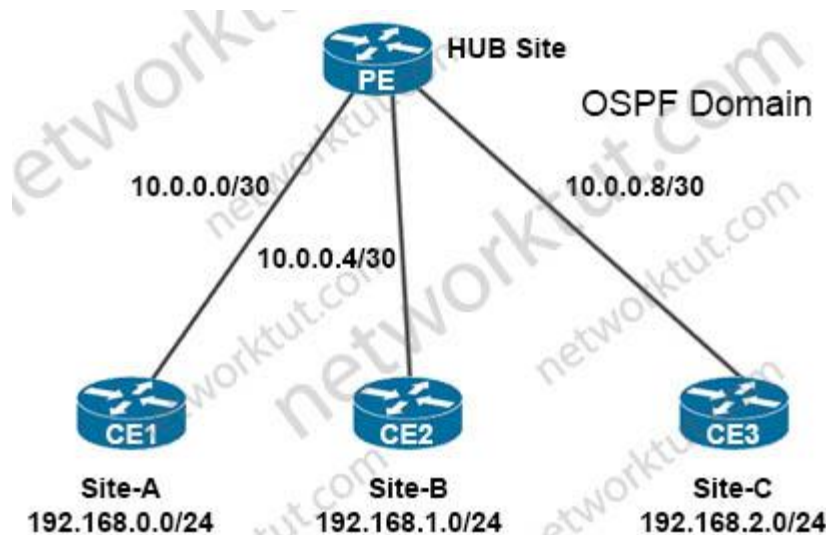
was notified that user 3 cannot even **ping** user 9 anymore. Where must the access list be applied in the outgoing direction to resolve the issue?

- A. R2 interface G0/0
- B. SW1 interface G1/10
- C. R2 interface G1/0
- D. SW1 interface G2/21

**Answer: C**

#### Question 4

Refer to the exhibit.



A network engineer must establish communication between three different customer sites with these requirements:

- Site-A must be restricted to access to any users at Site-B or Site-C.
- Site-B and Site-C: must be able to communicate between sites and share routes using OSPF

PE interface configuration:

```
interface FastEthernet0/0
 ip vrf forwarding Site-A
!
interface FastEthernet0/1
 ip vrf forwarding SharedSites
!
interface FastEthernet0/2
 ip vrf forwarding SharedSites
```

Which configuration meets the requirements?

- A. PE(config)#router ospf 10 vrf Site-A  
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0

```
PE(config)#router ospf 10 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 1
```

```
B. PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config-router)#router ospf 20 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 1
```

```
C. PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 10 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
```

```
D. PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 20 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
```

**Answer: C**

### Question 5

What is LDP label binding?

- A. destination prefix with label
- B. two routers with label distribution session
- C. source prefix with label
- D. neighboring router with label

**Answer: A**

### Question 6

Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 name ISP2 track 1
```

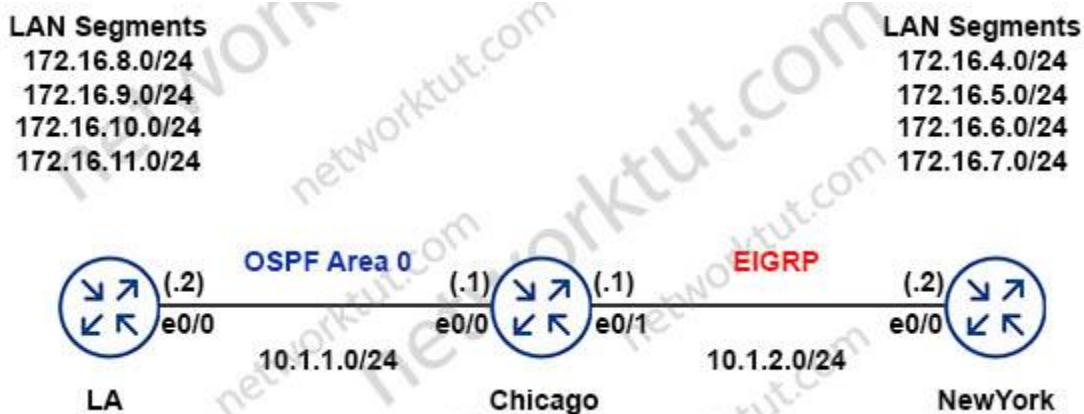
An administrator configures a router to stop using a particular default route if the DNS server 8.8.8.8 is not reachable through that route. However, this configuration did not work as desired and the default route still works even if the DNS server 8.8.8.8 is unreachable. Which two configuration changes resolve the issue? (Choose two)

- A. Use a separate track object to reference the existing IP SLA 1 probe for every static route
- B. Use a separate IP SLA probe and track object for every static route
- C. Associate every IP SLA probe with the proper WAN address of the router
- D. Reference the proper exit interfaces along with the next hops in both static default routes
- E. Configure two static routes for the 8.8.8.8/32 destination to match the IP SLA probe for each ISP

**Answer:** C D

### Question 7

Refer to the exhibit.



The network administrator configured the Chicago router to mutually redistribute the LA and New York routes with OSPF routes to be summarized as a single route in EIGRP using the longest summary mask:

```
router eigrp 100
 redistribute ospf 1 metric 10 10 10 10 10
router ospf 1
 redistribute eigrp 100 subnets
!
interface E 0/0
 ip summary-address eigrp 100 172.16.0.0 255.255.0.0
```

After the configuration, the New York router receives all the specific LA routes but the summary route. Which set of configurations resolves the issue on the Chicago router?

- A. router eigrp 100  
summary-address 172.16.8.0 255.255.252.0

B. interface E 0/1  
ip summary-address eigrp 100 172.16.8.0 255.255.252.0

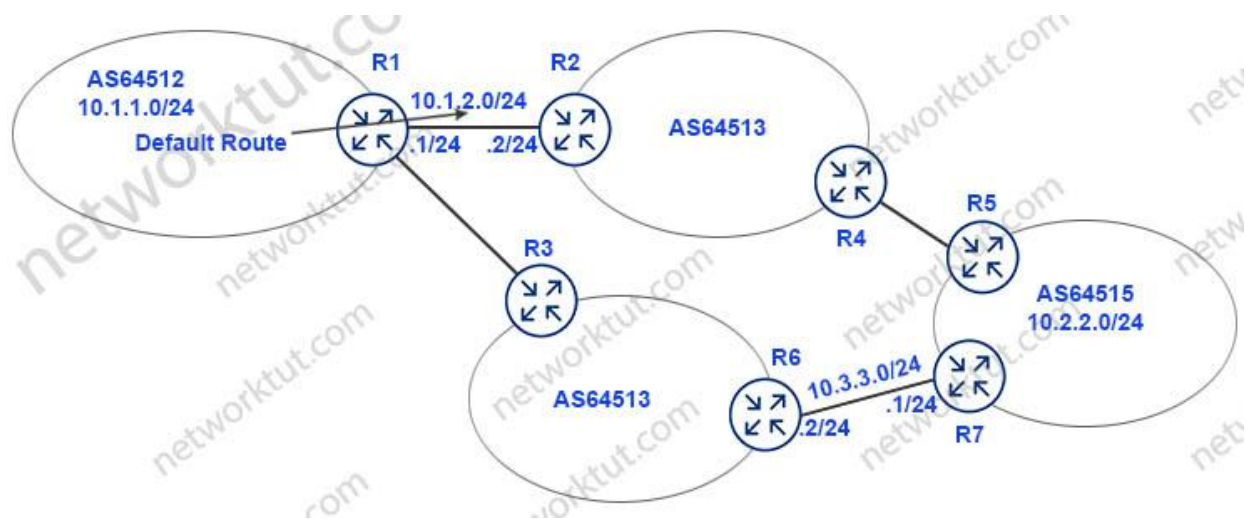
C. router eigrp 100  
summary-address 172.16.0.0 255.255.0.0

D. interface E 0/1  
ip summary-address eigrp 100 172.16.0.0 255.255.0.0

**Answer: B**

### Question 8

Refer to the exhibit.



An engineer must configure PBR on R1 to reach to 10.2.2.0/24 via R3 AS64513 as the primary path and a backup route through default route via R2 AS64513. All BGP routes are in the routing table of R1, but a static default route overrides BGP routes. Which PBR configuration achieves the objective?

A. access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255

!

route-map PBR permit 10

match ip address 100

set ip next-hop recursive 10.3.3.1

B. access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

!

route-map PBR permit 10

match ip address 100

set ip next-hop recursive 10.3.3.1

C. access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255

!

route-map PBR permit 10

match ip address 100

set ip next-hop 10.3.3.1

D. access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

!

route-map PBR permit 10

match ip address 100

set ip next-hop 10.3.3.1

**Answer: A**

### Question 9

What is the function of BFD?

A. It creates high CPU utilization on hardware deployments

B. It provides uniform failure detection on the same media type

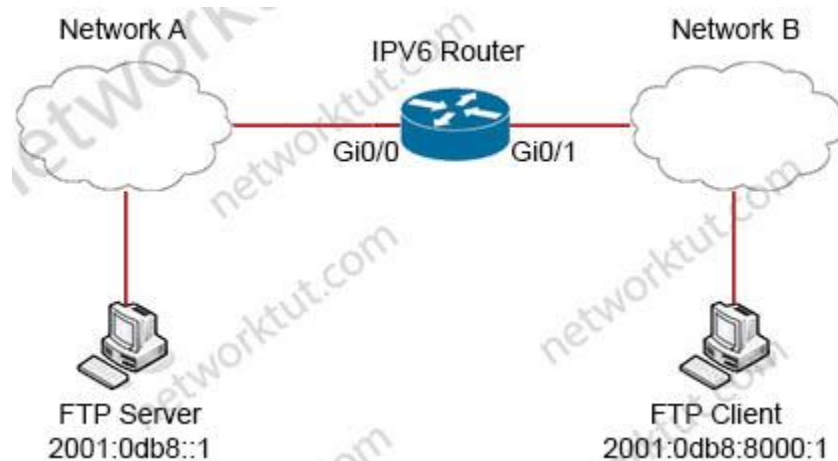
C. It provides uniform failure detection regardless of media type

D. It negotiates to the highest version if the neighbor version differs

**Answer: C**

### Question 10

Refer to the exhibit.



```
interface GigabitEthernet0/0
description FTP SERVER
no ip address
ipv6 address 2001:DB8::F/33
```

```

ipv6 enable
ipv6 traffic-filter FTP-SERVER in
!
interface GigabitEthernet0/1
description FTP CLIENT
no ip address
ipv6 address 2001:DB8:8000::F/33
ipv6 enable
ipv6 traffic-filter FTP-CLIENT in

ipv6 access-list FTP-CLIENT
permit tcp host 2001:DB8:8000::1 host 2001:DB8::1 eq ftp
permit tcp host 2001:DB8:8000::1 host 2001:DB8::1 eq ftp-data
!
ipv6 access-list FTP-SERVER
permit tcp host 2001:DB8::1 host 2001:DB8:8000::1 eq ftp established
permit tcp host 2001:DB8::1 host 2001:DB8:8000::1 eq ftp-data established

```

When an FTP client attempts to use passive FTP to connect to the FTP server, the file transfers fail. Which action resolves the issue?

- A. Modify traffic filter FTP-SERVER in to the outbound direction.
- B. Configure active FTP traffic
- C. Configure to permit TCP ports higher than 1023.
- D. Modify FTP-SERVER access list to remove established at the end.

**Answer: D**

### Question 11

Refer to the exhibit.

#### Configuration output:

```

aaa new-model
aaa group server tacacs+ admin
server name admin
!
ip tacacs source-interface GigabitEthernet1
aaa authentication login admin group tacacs+ local enable
aaa session-id common
!
tacacs server admin
address ip 10.11.15.6
key 7 01150F165E3C17032D
!
line vty 0 4
login authentication admin

```

#### Debug Output:



```

Oct 22 12:38 57 587 AAA/BIND(0000001A): Bind I/f
Oct 22 12:38:57.587: AAA/AUTHEN/LOGIN (0000001A) Pick method list 'admin'
Oct 22 12:38:57 587: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:38 57 587: AAA/AUTHEN/ENABLE(0000001A): Done status GET_PASSWORD
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Done status FAIL – bad password

```

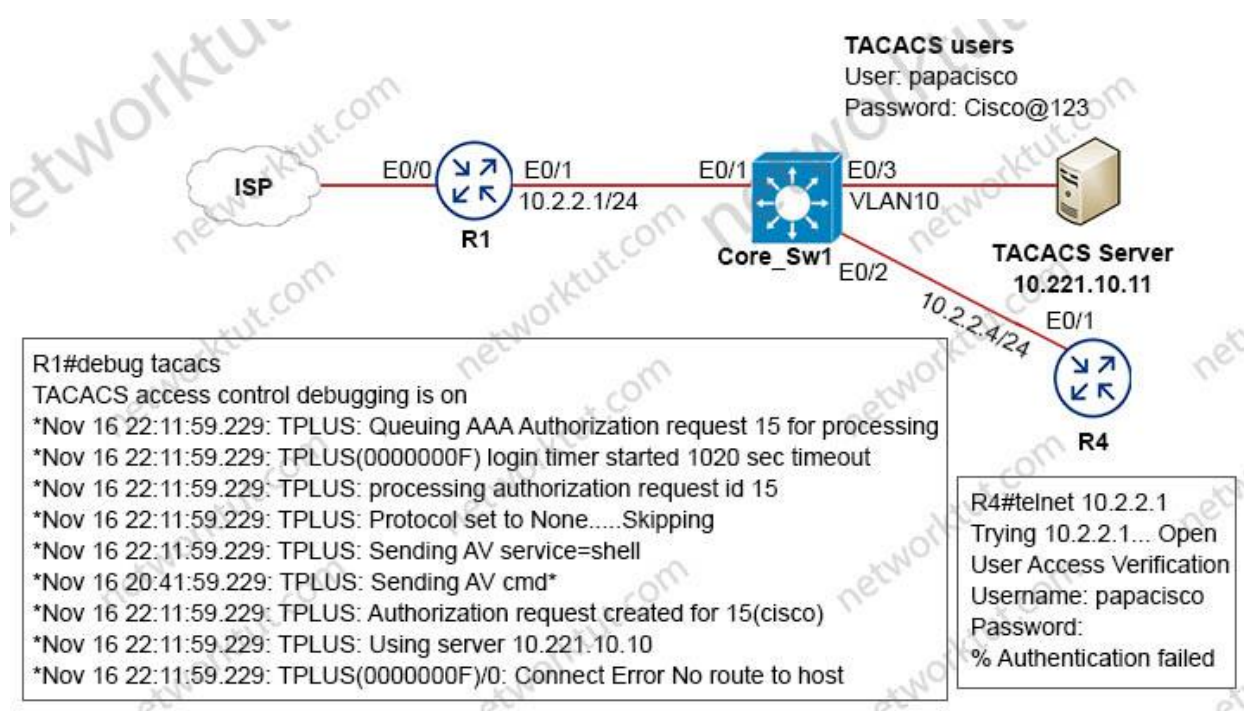
An administrator configured a Cisco router for TACACS authentication, but the router is using the local enable password instead. Which action resolves the issue?

- A. Configure the **aaa authentication login default group admin local if-authenticated** command instead.
- B. Configure the **aaa authentication login admin group tacacs+ local enable none** command instead.
- C. Configure the **aaa authentication login admin group tacacs+ local if-authenticated** command instead.
- D. Configure the **aaa authentication login admin group admin local enable command** instead.

**Answer: C**

## Question 12

Refer to the exhibit.



An engineer is trying to connect to R1 via Telnet with no success. Which configuration resolves the issue?

A. tacacs server prod  
address ipv4 10.221.10.11  
exit  
B. ip route 10.221.0.11 255.255.255.255 ethernet 0/1  
C. ip route 10.221.10.10 255.255.255.255 ethernet 0/1  
D. tacacs server prod  
address ipv4 10.221.10.10  
exit

**Answer: A**

### Question 13

An administrator attempts to download the pack NBAR2 file using TFTP from the CPE router to another device over the Gi0/0 interface. The CPE is configured as below:

```
hostname CPE
!
ip access-list extended WAN
<...>
remark => All UDP rules below for WAN ID: S421T18E58F90
permit udp any eq domain any
permit udp any any eq tftp
deny udp any any
!
interface GigabitEthernet0/0
<...>
ip access-group WAN in
<..>
!
tftp-server flash: pp-adv-csr1000v-1612.1a-37-53.0.0.pack
```

The transfer fails. Which action resolves this issue?

- A. Make the **permit udp any eq tftp any** entry the last entry in the WAN ACL
- B. Shorten the file name to the 8+3 naming convention.
- C. Change the WAN ACL to permit the entire UDP destination port range
- D. Change the WAN ACL to permit the UDP port 69 to allow TFTP.

**Answer: C**

### Question 14

A network administrator must optimize the segment size of the TCP packet on the DMVPN IPsec protected tunnel interface, which carries application traffic from the head office to a designated branch. The TCP segment size must not overwhelm the MTU of the outbound link. Which configuration must be applied to the router to improve the application performance?

A. interface tunnel30  
ip mtu 1400  
ip tcp payload-size 1360  
!  
crypto ipsec fragmentation before-encryption

B. interface tunnel30  
ip mtu 1400  
ip tcp adjust-mss 1360  
!  
crypto ipsec fragmentation after-encryption

C. interface tunnel30  
ip mtu 1400  
ip tcp max-segment 1360  
!  
crypto ipsec fragmentation before-encryption

D. interface tunnel30  
ip mtu 1400  
ip tcp packet-size 1360  
!  
crypto ipsec fragmentation after-encryption

**Answer: A**

### **Question 15**

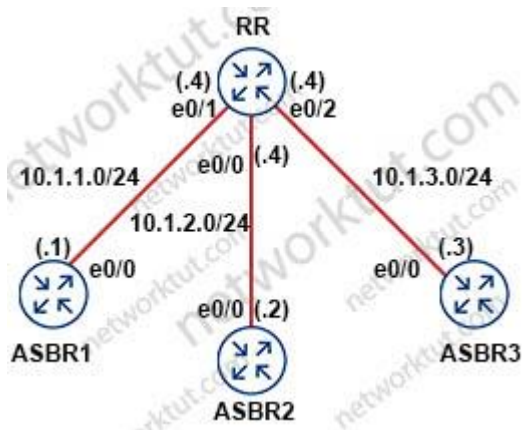
In a DMVPN network, the Spoke1 user observed that the voice traffic is coming to Spoke2 users via the hub router. Which command is required on both spoke routers to communicate directly to one another?

- A. ip nhrp nhs multicast
- B. ip nhrp shortcut
- C. ip nhrp map dynamic
- D. ip nhrp redirect

**Answer: B**

### **Question 16**

Refer to the exhibit.



**RR Configuration:**

```
router bgp 100
neighbor IBGP peer-group
neighbor IBGP route-reflector-client
neighbor 10.1.1.1 remote-as 100
neighbor 10.1.2.2 remote-as 100
neighbor 10.1.3.3 remote-as 100
```

The network administrator configured the network to establish connectivity between all devices and notices that the ASBRs do not have routes for each other. Which set of configurations resolves this issue?

A. router bgp 100  
neighbor IBGP update-source Loopback0

B. router bgp 100  
neighbor IBGP next-hop-self

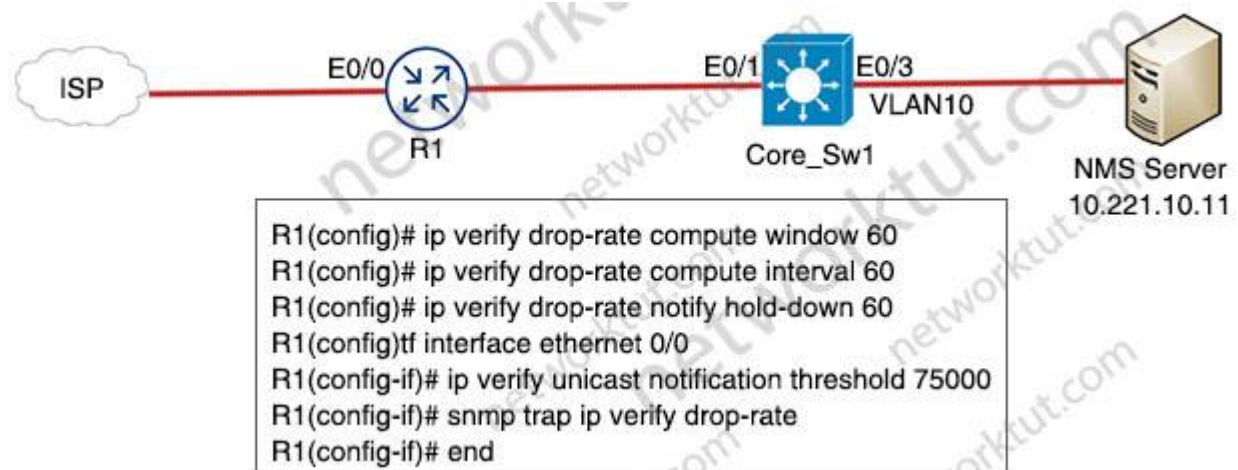
C. router bgp 100  
neighbor 10.1.1.1 next-hop-self  
neighbor 10.1.2.2 next-hop-self  
neighbor 10.1.3.3 next-hop-self

D. router bgp 100  
neighbor 10.1.1.1 peer-group IBGP  
neighbor 10.1.2.2 peer-group IBGP  
neighbor 10.1.3.3 peer-group IBGP

**Answer: D**

**Question 17**

Refer to the exhibit.



An engineer configured SNMP traps to record spoofed packets drop of more than 48000 a minute on the ethernet0/0 interface. During an IP spoofing attack, the engineer noticed that no notifications have been received by the SNMP server. Which configuration resolves the issue on R1?

- A. ip verify unicast notification threshold 800
- B. ip verify unicast notification threshold 8000
- C. ip verify unicast notification threshold 48000
- D. ip verify unicast notification threshold 80

**Answer: A**

### Question 18

Refer to the exhibit.

```

R1:
interface Loopback1
no ip address
ipv6 address 100A:0:100C::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Loopback4
no ip address
ipv6 address 400A:0:400C::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Serial1/0
no ip address
ipv6 address AB01:2011:7:100::/64 eui-64
ipv6 enable
ipv6 ospf network point-to-point
ipv6 ospf 10 area 0
ipv6 traffic-filter DENY_TELNET_Lo4 in
serial restart-delay 0
clock rate 64000
!
ipv6 router ospf 10
router-id 1.1.1.1
log-adjacency-changes
!
ipv6 access-list DENY_TELNET_LO4
sequence 20 deny tcp host 100:ABC:2011:7 host 400A:0:400C::1 eq telnet permit ipv6 any any
end

R2:
interface Loopback0
no ip address
ipv6 address 1001:ABC:2011:7::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Serial1/0
no ip address
ipv6 address AB01:2011:7:100::/64 eui-64
ipv6 enable
ipv6 ospf network point-to-point
ipv6 ospf 10 area 0
serial restart-delay 0
!
ipv6 router ospf 10
router-id 2.2.2.2
log-adjacency-changes
!
end

```

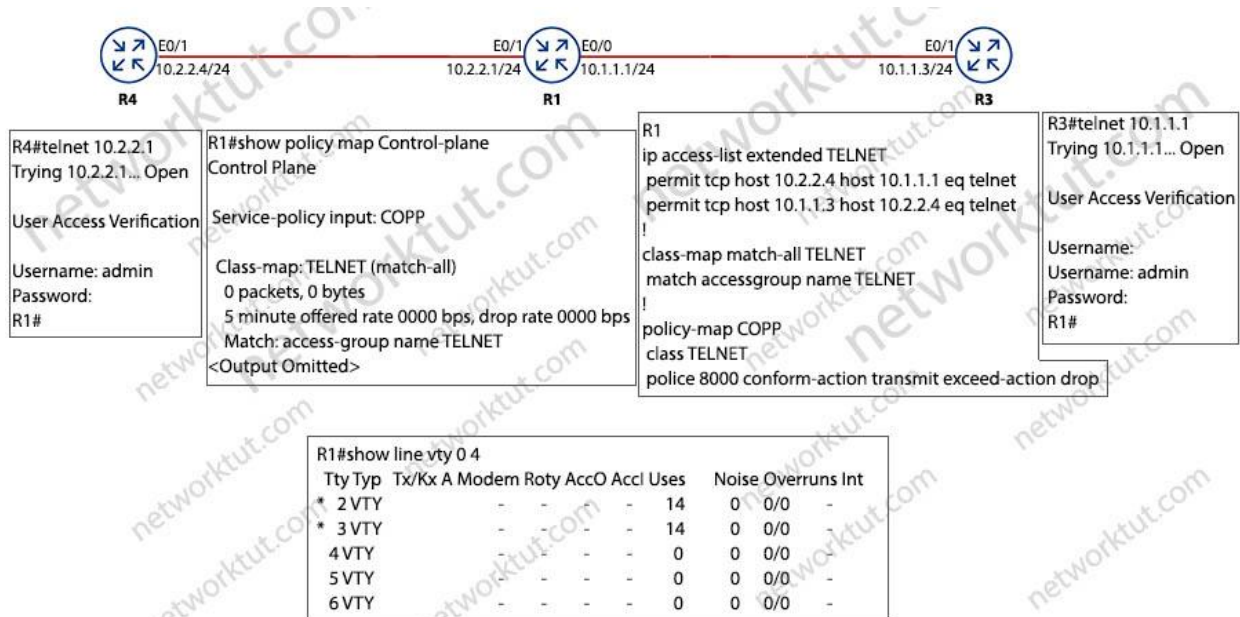
An engineer implemented an access list on R1 to allow anyone to Telnet except R2 Loopback0 to R1 Loopback4. How must sequence 20 be replaced on the R1 access list to resolve the issue?

- A. sequence 20 permit tcp host 1001:ABC:2011:7::1 host 400A:0:400C::1 eq telnet
- B. sequence 20 deny tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet
- C. sequence 20 permit tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet
- D. sequence 20 deny tcp host 1001:ABC:2011:7::1 host 400A:0:400C::1 eq telnet

**Answer: D**

### Question 19

Refer to the exhibit.



An engineer implemented CoPP to limit Telnet traffic to protect the router CPU. It was noticed that the Telnet traffic did not pass through CoPP. Which configuration resolves the issue?

A. ip access-list extended TELNET

permit tcp host 10.2.2.1 host 10.2.2.4 eq telnet

permit tcp host 10.1.1.1 host 10.1.1.3 eq telnet

B. policy-map COPP

class TELNET

police 8000 conform-action transmit exceed-action transmit

C. ip access-list extended TELNET

permit tcp host 10.2.2.4 host 10.2.2.1 eq telnet

permit tcp host 10.1.1.3 host 10.1.1.1 eq telnet

D. policy-map COPP

class TELNET

police 8000 conform-action transmit exceed-action transmit violate-action drop

**Answer: C**

**Question 20**

Refer to the exhibit.

# R1# show ip ospf database self-originate

OSPF Router with ID (10.255.255.1) (Process ID 1)

## Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
Link count				
10.255.255.1	10.255.255.1	4	0x8000038D	0x001AD9
3				

## Summary Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.0.34.0	10.255.255.1	3604	0x80000380	0x00275C
10.255.255.4	10.255.255.1	3604	0x80000380	0x00762B

## Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum
Tag				
0.0.0.0	10.255.255.1	3604	0x800001D0	0x001CBC
0				

\*Feb 22 22:50:39.523: %OSPF-4-FLOOD\_WAR: Process 1 flushes LSA  
ID 0.0.0.0 type-5 adv-rtr 10.255.255.1 in area 0

After configuring OSPF in R1, some external destinations in the network became unreachable.  
Which action resolves the issue?

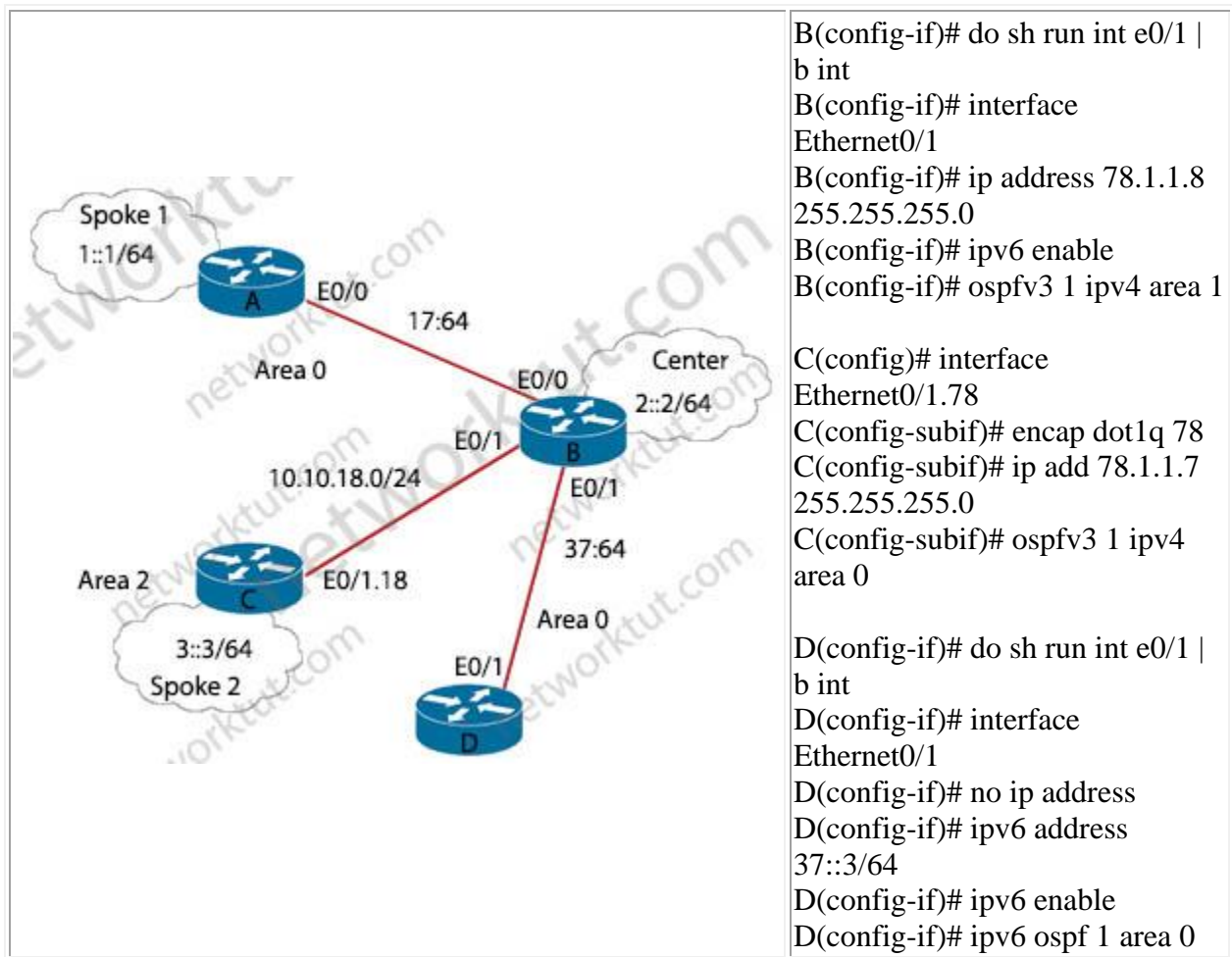
- A. Disconnect the router with the OSPF router ID 0.0.0.0 from the network
- B. Increase the SPF delay interval on R1 to synchronize routes.
- C. Change the R1 router ID from 10.255.255.1 to a unique value and clear the process
- D. Clear the OSPF process on R1 to flush stale LSAs sent by other routers

**Answer: C**

## Question 21

Refer to the exhibit.





A network engineer receives a report that Spoke 1 users can perform bank transactions with the server located at the Center site, but Spoke 2 users cannot. Which action resolves the issue?

- A. Configure the Spoke 2 users IP on the router B OSPF domain.
- B. Configure IPv6 on the routers B and C interfaces.
- C. Configure OSPFv2 on the routers B and C interfaces.
- D. Configure encapsulation dot1q 78 on the router C interface.

**Answer: C**

## Question 22

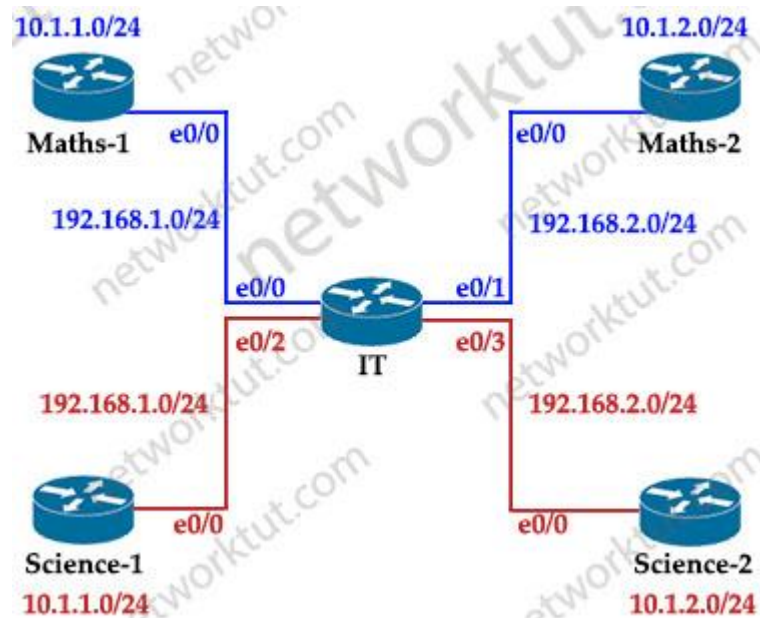
What is an MPLS LDP targeted session?

- A. LDP session established by exchanging multicast hello packets
- B. LDP session established between LSRs by exchanging TCP hello packets
- C. session between neighbors that are connected no more than one hop away
- D. label distribution session between non-directly connected neighbors

Answer: D

### Question 23

Refer to the exhibit.



```
IT Router
vrf definition Science
address-family ipv4
!
interface E 0/2
Vrf forwarding Science
ip address 192.168.1.1 255.255.255.0
No shut
!
Interface E 0/3
Vrf forwarding Science
ip address 192.168.2.1 255.255.255.0
No shut
```

The IT router has been configured with the Science VRF and the interfaces have been assigned to the VRF. Which set of configurations advertises Science-1 and Science-2 routes using EIGRP AS 111?

#### Option A

```
router eigrp 111
address-family ipv4 vrf Science autonomous-
system 1
network 192.168.1.0
```

#### Option B

```
router eigrp 111
address-family ipv4 vrf Science
network 192.168.1.0
network 192.168.2.0
```

network 192.168.2.0	
<b>Option C</b>  router eigrp 111 network 192.168.1.0 network 192.168.2.0	<b>Option D</b>  router eigrp 1 address-family ipv4 vrf Science autonomous-system 111 network 192.168.1.0 network 192.168.2.0

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

#### Question 24

An engineer must override the normal routing behavior of a router for Telnet traffic that is destined to 10.10.10.10 from 10.10.1.0/24 via a next hop of 10.4.4.4, which is directly connected to the router that is connected to the 10.1.1.0/24 subnet. Which configuration reroutes traffic according to this requirement?

<b>Option A</b>  access-list 100 deny tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23 ! route-map POLICY permit 10 match ip address 100 set ip next-hop 10.4.4.4 route-map POLICY permit 20	<b>Option B</b>  access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23 ! route-map POLICY permit 10 match ip address 100 set ip next-hop 10.4.4.4 route-map POLICY permit 20
<b>Option C</b>  access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23 ! route-map POLICY permit 10 match ip address 100 set ip next-hop recursive 10.4.4.4 route-map POLICY permit 20	<b>Option D</b>  access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23 ! route-map POLICY permit 10 match ip address 100 set ip next-hop recursive 10.4.4.4

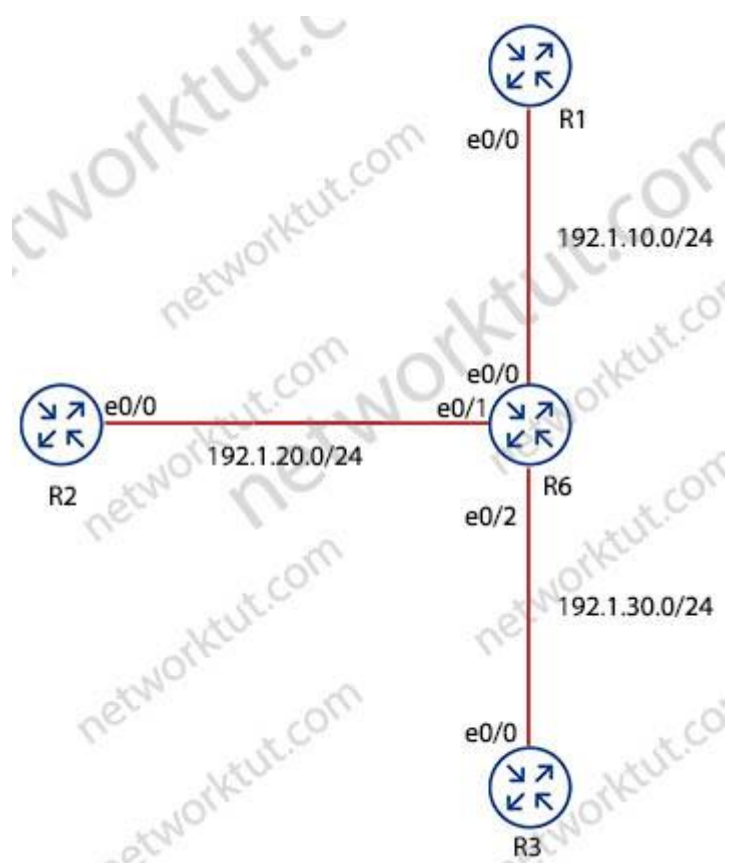
- A. Option A
- B. Option B

- C. Option C
- D. Option D

**Answer: B**

### Question 25

Refer to the exhibit.



An engineer must configure DMVPN Phase 3 hub-and-spoke topology to enable a spoke-to-spoke tunnel. Which NHRP configuration meets the requirement on R6?

- A. interface Tunnel1  
ip nhrp authentication Cisco123  
ip nhrp map multicast dynamic  
ip nhrp network-id 1  
ip nhrp holdtime 300  
ip nhrp redirect
- B. interface Tunnel 1  
ip address 192.168.1.1 255.255.255.0  
tunnel source e 0/1  
tunnel mode gre multipoint

```
ip nhrp network-id 1
ip nhrp map 192.168.1.2 192.1.20.2
```

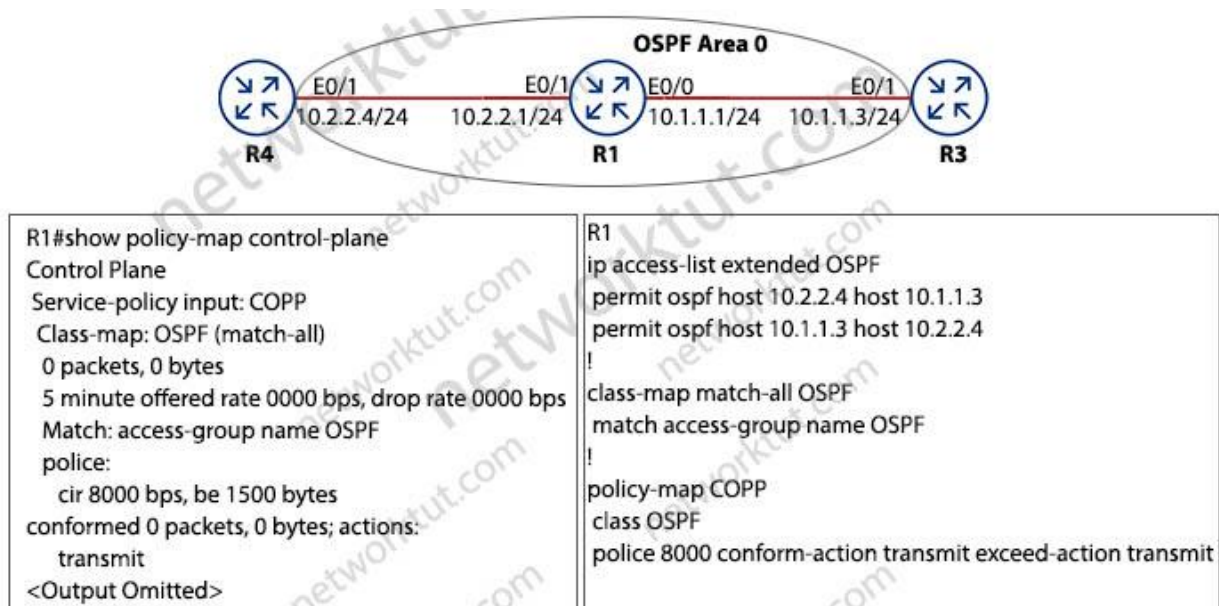
```
C. interface Tunnel1
ip nhrp authentication Cisco123
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp shortcut
```

```
D. interface Tunnel 1
ip address 192.168.1.1 255.255.255.0
tunnel source e 0/0
tunnel mode gre multipoint
ip nhrp network-id 1
```

**Answer: A**

## Question 26

Refer to the exhibit.



An engineer implemented CoPP but did not see OSPF traffic going through it. Which configuration resolves the issue?

```
A. control-plane
service-policy input COPP
```

B. policy-map COPP

class OSFP

police 8000 conform-action transmit exceed-action transmit violate-action drop

C. ip access-list extended OSPF

permit ospf any any

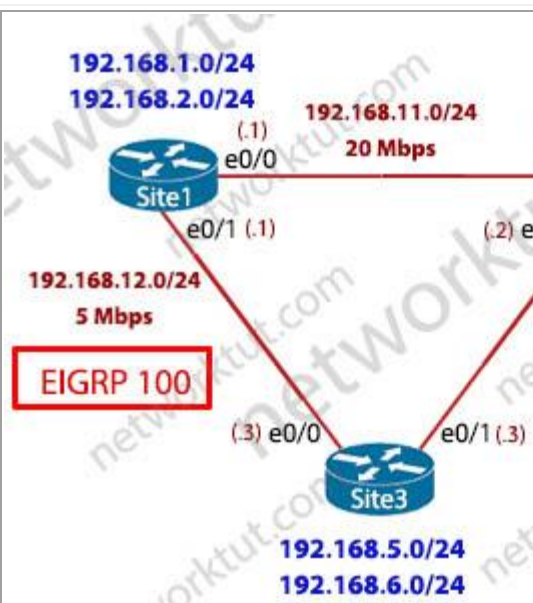
D. class-map match-all OSFP

match access-group name OSPF

**Answer: C**

### **Question 27**

Refer to the exhibit.



#### Site1 - Show ip route

Gateway of last resort is not set

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, Loopback0
L    192.168.1.1/32 is directly connected, Loopback0
D    192.168.3.0/24 [90/281600] via 192.168.11.2, 00:00:23
D    192.168.4.0/24 [90/281600] via 192.168.11.2, 00:00:23
D    192.168.5.0/24 [90/665600] via 192.168.12.3, 00:00:23
        [90/435200] via 192.168.11.2, 00:00:23
D    192.168.6.0/24 [90/665600] via 192.168.12.3, 00:00:23
        [90/435200] via 192.168.11.2, 00:00:23
192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.11.0/24 is directly connected, Ethernet0/0
L    192.168.11.1/32 is directly connected, Ethernet0/0
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/24 is directly connected, Ethernet0/1
L    192.168.12.1/32 is directly connected, Ethernet0/1
D    192.168.13.0/24 [90/563200] via 192.168.12.3, 00:00:23
        [90/307200] via 192.168.11.2, 00:00:23, Et
  
```

#### Site1 - Show ip eigrp topology

```

P 192.168.3.0/24, 1 successors, FD is 230400
    via 192.168.11.2 (281600/128256), Ethernet0/0
    via 192.168.12.3 (691200/204800), Ethernet0/1
P 192.168.12.0/24, 1 successors, FD is 537600
    via Connected, Ethernet0/1
P 192.168.13.0/24, 2 successors, FD is 307200
    via 192.168.12.3 (563200/76800), Ethernet0/1
    via 192.168.11.2 (307200/281600), Ethernet0/0
P 192.168.1.0/24, 1 successors, FD is 128256
    via Connected, Loopback0
P 192.168.6.0/24, 2 successors, FD is 435200
    via 192.168.12.3 (665600/128256), Ethernet0/1
    via 192.168.11.2 (435200/409600), Ethernet0/0
P 192.168.4.0/24, 1 successors, FD is 230400
    via 192.168.11.2 (281600/128256), Ethernet0/0
    via 192.168.12.3 (691200/204800), Ethernet0/1
P 192.168.5.0/24, 2 successors, FD is 435200
    via 192.168.12.3 (665600/128256), Ethernet0/1
    via 192.168.11.2 (435200/409600), Ethernet0/0
P 192.168.11.0/24, 1 successors, FD is 153600
    via Connected, Ethernet0/0
  
```

#### Site1 - Show run | section router

```

router eigrp 100
 variance 2
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.11.0
 network 192.168.12.0
  
```



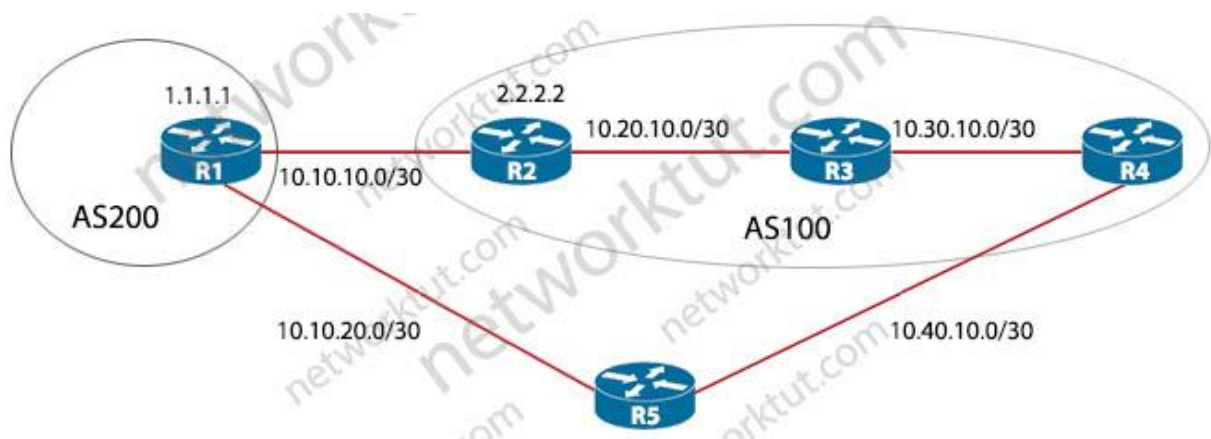
Site1 must perform unequal cost load balancing toward the segments behind Site2 and Site3. Some of the routes are getting load balanced but others are not. Which configuration allows Site1 to load balance toward all the LAN segments of the remote routers?

- A. Site3  
router eigrp 100  
variance 2
- B. Site2  
router eigrp 100  
variance 2
- C. Site2  
router eigrp 100  
variance 3
- D. Site1  
router eigrp 100  
variance 3

**Answer: D**

### Question 28

Refer to the exhibit.



R2# router eigrp 100 network 10.10.10.0 0.0.0.3 network 10.20.10.0 0.0.0.3 ! router ospf 100	R1# router eigrp 100 network 10.10.10.0 0.0.0.3 network 10.10.20.0 0.0.0.3 network 1.1.1.1 0.0.0.0 !
---	---



<pre> network 10.10.10.0 0.0.0.3 area 0 network 10.20.10.0 0.0.0.3 area 0 ! ! ! router bgp 100 distance 100 10.20.10.0 0.0.0.3 distance 100 10.10.10.0 0.0.0.3 neighbor 1.1.1.1 remote-as 200 neighbor 10.10.10.1 remote-as 200 network 10.20.10.0 mask 255.255.255.252 </pre>	<pre> router ospf 100  network 10.10.10.0 0.0.0.3 area 0 network 10.10.20.0 0.0.0.3 area 0 ! router bgp 200 distance 100 10.10.10.0 0.0.0.3 distance 100 10.20.10.0 0.0.0.3 neighbor 2.2.2.2 remote-as 100 neighbor 10.10.10.2 remote-as 100 network 10.10.10.0 mask 255.255.255.252 network 10.20.10.0 mask 255.255.255.252 </pre>
--	---

R1 and R2 use IGP protocol to route traffic between AS 100 and AS 200 despite being configured to use BGP. Which action resolves the issue and ensures the use of BGP?

- A. Configure distance to 100 under the OSPF process of R1 and R2.
- B. Remove distance commands under BGP AS 100.
- C. Remove distance commands under BGP AS 100 and AS 200.
- D. Configure distance to 100 under the EIGRP process of R1 and R2.

**Answer: C**

### Question 29

Refer to the exhibit.

```
R1#show cef inter e0/0
```

```
Ethernet0/0 is up (if_number 3)
```

```
Corresponding hwidb fast_if_number 3
```

```
Corresponding hwidb firstsw->if_number 3
```

```
Internet address is 209.165.200.226/30
```

```
ICMP redirects are always sent
```

```
Per packet load-sharing is disabled
```

```
IP unicast RPF check is enabled
```

```
Input features: uRPF
```

```
IP policy routing is disabled
```

```
<Output Omitted>
```

```
R1#show cef inter e0/1
```

```
Ethernet0/1 is up (if_number 4)
```

```
Corresponding hwidb fast_if_number 4
```

```
Corresponding hwidb firstsw->if_number 4
```

```
Internet address is 209.165.201.2/30
```

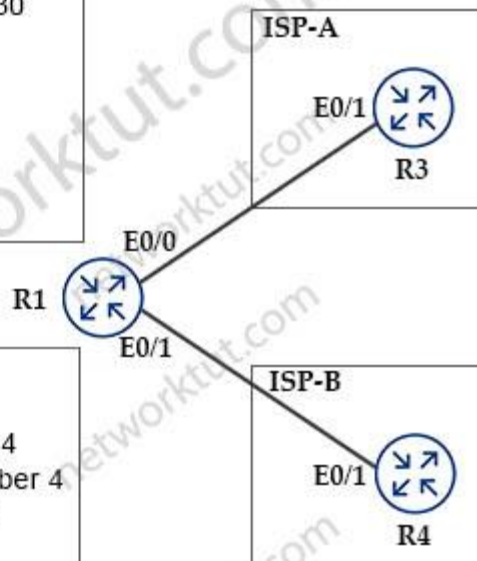
```
ICMP redirects are always sent
```

```
Per packet load-sharing is disabled
```

```
IP unicast RPF check is disabled
```

```
IP policy routing is disabled
```

```
<Output Omitted>
```



### Regional Data Center

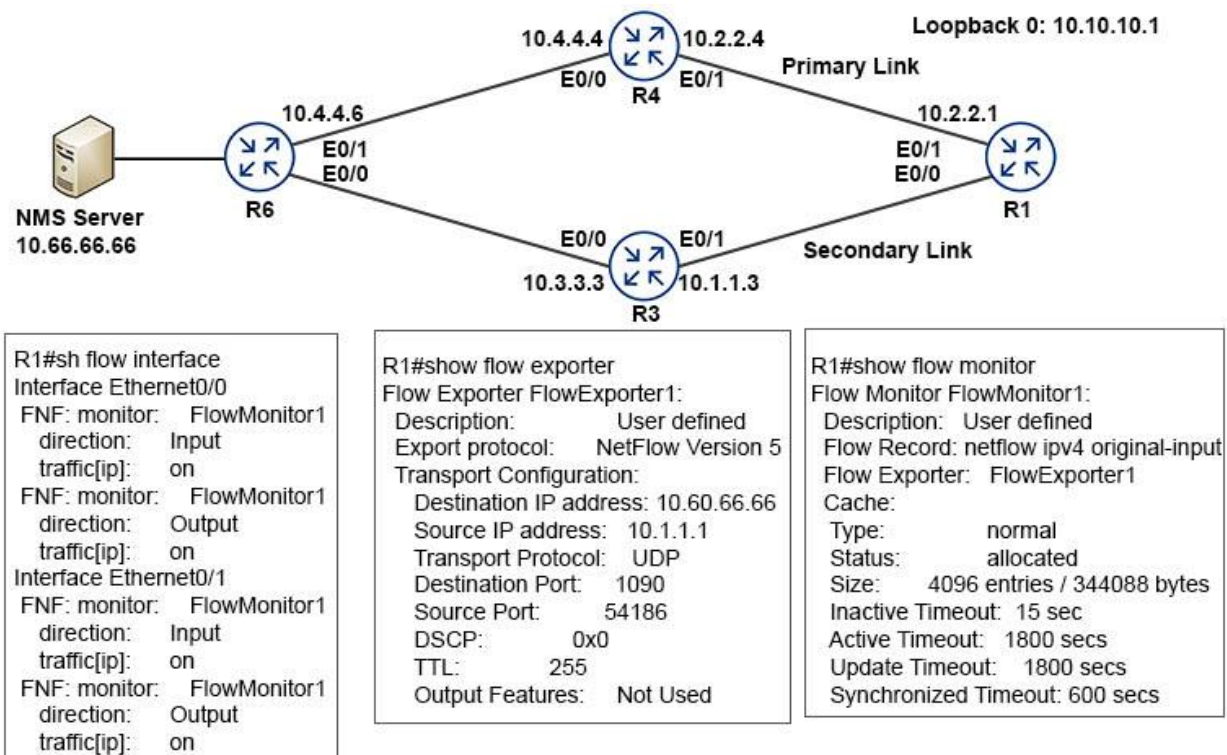
The company implemented uRPF to address an antispoofing attack. A network engineer received a call from the IT security department that the regional data center is under an IP attack. Which configuration must be implemented on R1 to resolve this issue?

- A. interface ethernet0/0  
ip verify unicast reverse-path
- B. interface ethernet0/1  
ip verify unicast reverse-path
- C. interface ethernet0/1  
ip unicast RPF check reachable-via any allow-default allow-self-ping
- D. interface ethernet0/0  
ip unicast RPF check reachable-via any allow-default allow-self-ping

**Answer: B**

### Question 30

Refer to the exhibit.



An engineer configured NetFlow on R1, but the flows do not reach the NMS server from R1. Which configuration resolves this issue?

- A. R1(config)#flow monitor FlowMonitor1  
R1(config-flow-monitor)#destination 10.66.66.66
- B. R1(config)#flow exporter FlowExporter1  
R1(config-flow-monitor)#destination 10.66.66.66
- C. R1(config)#interface Ethernet0/0  
R1(config-if)#ip flow monitor Flowmonitor1 input  
R1(config-if)#ip flow monitor Flowmonitor1 output
- D. R1(config)#interface Ethernet0/1  
R1(config-if)#ip flow monitor Flowmonitor1 input  
R1(config-if)#ip flow monitor Flowmonitor1 output

**Answer: B**

### Question 31

Refer to the exhibit.

```

R1#sh run | section eigrp
router eigrp 10
network 10.10.10.0 0.0.0.255
no auto-summary
neighbor 10.10.10.2 FastEthernet0/0
neighbor 10.10.10.3 FastEthernet0/0

```

```

R1#show ip eigrp neighbors

```

```

IP-EIGRP neighbors for process 10
H   Address           Interface    Hold Uptime  SRTT  RTO   Q
Seq                                     (sec)      (ms)  Cnt

Num
1  10.10.10.2         Fa0/0       10 00:01:01   42 232   0 6
0  10.10.10.3         Fa0/0       10 00:01:03   43 244   0 6

```

The remote branch locations have a static neighbor relationship configured to R1. Only R1 has successful neighbor relationships with the remote locations of R2 and R3, but the end users cannot communicate with each other. Which configuration resolves the issue?

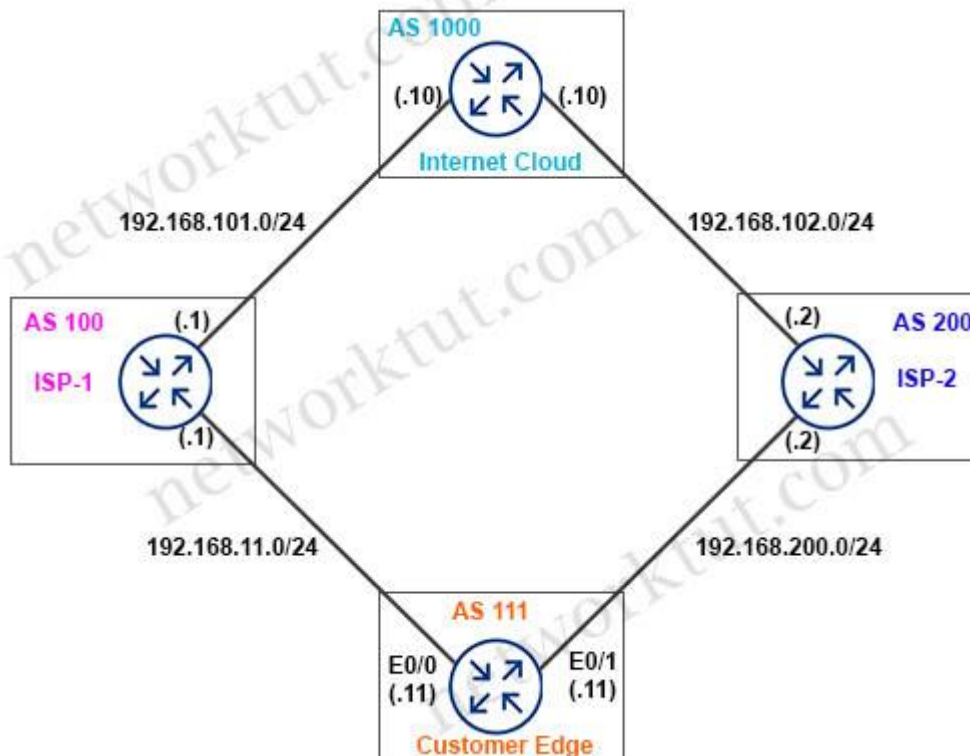
<b>Option A</b>  R2 and R3 interface FastEthernet0/0 no ip split-horizon eigrp 10	<b>Option B</b>  R2 interface FastEthernet0/0.10 encapsulation dot1Q 10 ip address 10.10.10.2 255.255.255.0  R3 interface FastEthernet0/0.10 encapsulation dot1Q 10 ip address 10.10.10.3 255.255.255.0
<b>Option C</b>  R1 interface FastEthernet0/0 no ip split-horizon eigrp 10	<b>Option D</b>  R2 interface FastEthernet0/0.10 encapsulation dot1Q ip address 10.10.10.2 255.255.255.0  R3 interface FastEthernet0/0.10 encapsulation dot1Q ip address 10.10.10.3 255.255.255.0

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

### Question 32

Refer to the exhibit.



AS 111 must not be used as a transit AS, but ISP-1 is getting ISP-2 routes from AS 111. Which configuration stops Customer AS from being used as a transit path on ISP-1?

- A. ip as-path access-list 1 permit ^ \$
- B. ip as-path access-list 1 permit \_111\_
- C. ip as-path access-list 1 permit ."
- D. ip as-path access-list 1 permit ^111\$

**Answer: A**

### Question 33

Refer to the exhibit.

```

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)

```

Which action limits the access to R2 from 192.168.12.1?

- 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**

### Question 34

A network administrator cannot connect to a device via SSH. The line vty configuration is as follows. Which action resolves this issue?

```

line vty 0 4
 location S421TE3483FG
 session-timeout 10
 transport preferred ssh
 transport input all
 transport output telnet ssh
 stopbits 1

```

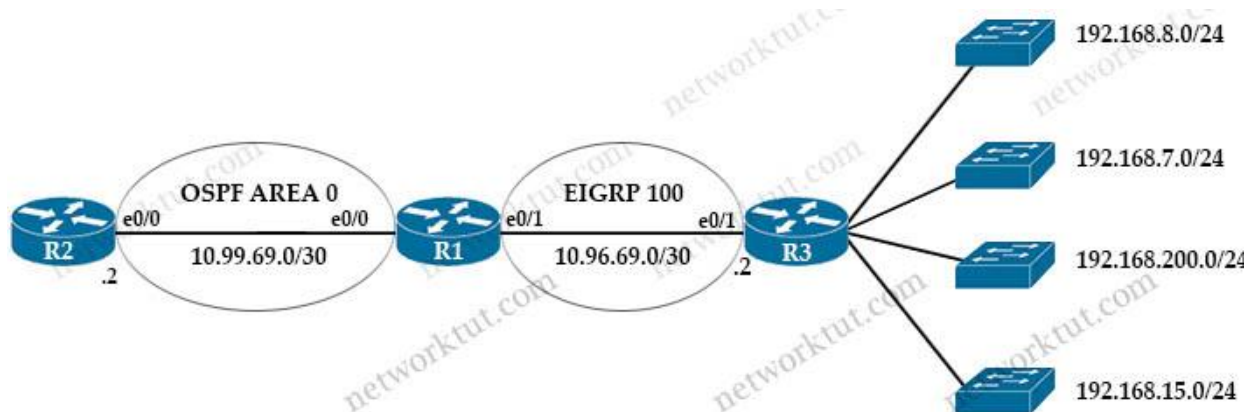
- A. Increase the session timeout
- B. Change the stopbits to 10

- C. Configure the transport input SSH
- D. Initialize the SSH key

**Answer: D**

### Question 35

Refer to the exhibit.



```
R1#show route-map

route map FROM->EIGRP, permit, sequence 10
  Match clauses:
    ip address (access-lists): 10
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
R1#show run | sec router
router eigrp 100
  network 10.96.69.0 0.0.0.3
  no auto-summary
  eigrp router-id 1.1.1.1
router ospf 100
  router-id 1.1.1.1
  log adjacency-changes
  redistribute eigrp 100 subnets route-map FROM->EIGRP
  network 10.99.69.0 0.0.0.3 area 0
R1#show ip access-list
Standard IP access list 10
  10 permit 192.168.16.0, wildcard bits 0.0.3.255
  11 permit 192.168.0.0, wildcard bits 0.0.7.255
  20 deny any
```

The engineer configured route redistribution in the network but soon received reports that R2 cannot access 192.168.7.0/24 and 192.168.15.0/24 subnets. Which configuration resolves the issue?

- A. R1(config)#ip access-list standard 10
- R1(config-std-nacl)#no 10 permit
- R1(config-std-nacl)#no 11 permit

```
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.3.255
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.3.255
```

B. R1(config)#ip access-list standard 10  
R1(config-std-nacl)#no 10 permit  
R1(config-std-nacl)#no 11 permit  
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.7.255  
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.3.255

C. R1(config)#ip access-list standard 10  
R1(config-std-nacl)#no 10 permit  
R1(config-std-nacl)#no 11 permit  
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.3.255  
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.7.255

D. R1(config)#ip access-list standard 10  
R1(config-std-nacl)#no 10 permit  
R1(config-std-nacl)#no 11 permit  
R1(config-std-nacl)#10 permit 192.168.4.0 0.0.3.255  
R1(config-std-nacl)#11 permit 192.168.12.0 0.0.3.255

**Answer: D**

### **Question 36**

Which table is used to map the packets in an MPLS LSP that exit from the same interface, via the same next hop, and have the same queuing policies?

- A. RIB
- B. FEC
- C. LDP
- D. CEF

**Answer: B**

### **Question 37**

Drag and drop the ICMPv6 neighbor discovery messages from the left onto the correct packet types on the right.



Neighbor Advertisement	ICMPv6 Type 134
Neighbor Solicitation	ICMPv6 Type 137
Redirect Message	ICMPv6 Type 135
Router Advertisement	ICMPv6 Type 133
Router Solicitation	ICMPv6 Type 136

**Answer:**

ICMPv6 Type 134: Router Advertisement

ICMPv6 Type 137: Redirect Message

ICMPv6 Type 135: Neighbor Solicitation

ICMPv6 Type 133: Router Solicitation

ICMPv6 Type 136: Neighbor Advertisement

### Question 38

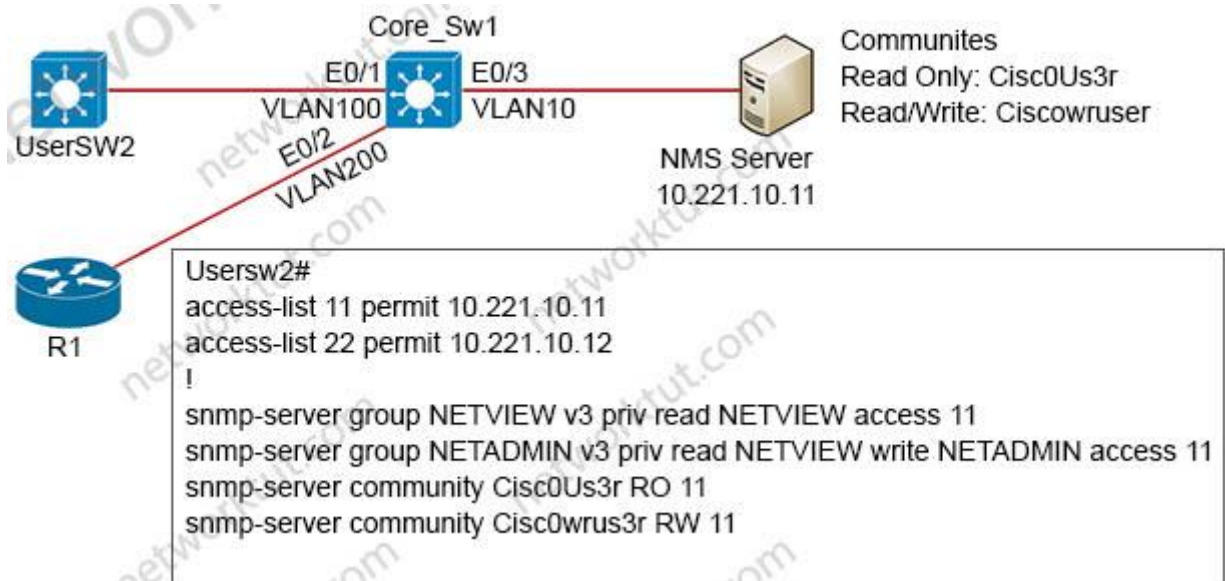
What is a function of BFD?

- A. peer recovery after a Layer 3 protocol adjacency failure
- B. peer recovery after a Layer 2 adjacency failure
- C. failure detection independent of routing protocols and media types
- D. failure detection dependent on routing protocols and media types

**Answer: C**

### Question 39

Refer to the exhibit.



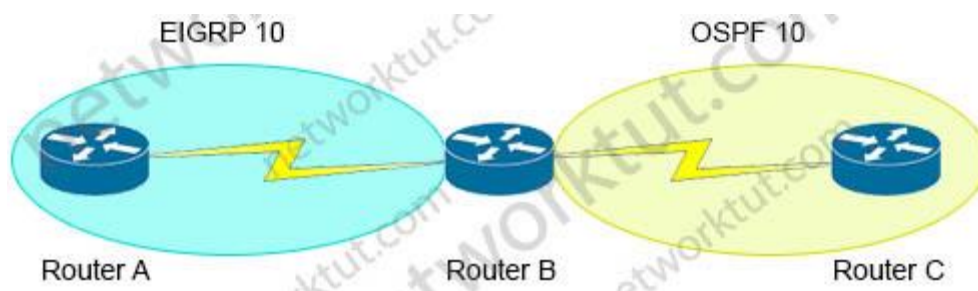
An engineer configured SNMP Communities on UserSW2 switch, but the SNMP server cannot upload modified configurations to the switch. Which configuration resolves this issue?

- A. snmp-server community Ciscowruser RW 11
- B. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
- C. snmp-server community Cisc0Us3r RW 11
- D. snmp-server group NETVIEW v2c priv read NETVIEW access 11

**Answer: A**

#### Question 40

Refer to the exhibit.



RouterB:

```

router eigrp CLASS
!
address-family ipv4 unicast autonomous-system 10
!
topology base
 redistribute ospf 10 match external 1 external 2 metric 1000000 10 255 1
1500
exit-af-topology
  
```

```

network 172.16.2.2 0.0.0.0
eigrp router-id 2.2.2.2
exit-address-family

```

```

172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.16.1.0/30 is directly connected, GigabitEthernet0/0
L      172.16.1.2/32 is directly connected, GigabitEthernet0/0
C      172.16.2.0/30 is directly connected, GigabitEthernet0/1
L      172.16.2.2/32 is directly connected, GigabitEthernet0/1
      192.168.0.0/32 is subnetted, 1 subnets
O      192.168.0.1 [110/2] via 172.16.1.1, 1d04h, GigabitEthernet0/0
      192.168.1.0/32 is subnetted, 1 subnets
O      192.168.1.1 [110/2] via 172.16.1.1, 1d04h, GigabitEthernet0/0
      192.168.2.20/32 is subnetted, 1 subnets
O      192.168.2.1 [110/2] via 172.16.1.1, 1d04h, GigabitEthernet0/0
D      192.168.11.0/24 [90/10880] via 172.16.2.1, 1d04h,
GigabitEthernet0/1
D      192.168.12.0/24 [90/10880] via 172.16.2.1, 1d04h,
GigabitEthernet0/1
D      192.168.13.0/24 [90/10880] via 172.16.2.1, 1d04h,
GigabitEthernet0/1

```

An engineer configured route exchange between two different companies for a migration project. EIGRP routes were learned in router C but no OSPF routes were learned in router A. Which configuration allows router A to receive OSPF routes?

- A. (config-router-af)#redistribute ospf 10 1000000 10 255 1 1500
- B. (config-router-af-topology)#redistribute ospf 10 metric 1000000 10 255 1 1500
- C. (config-router-af-topology)#redistribute connected
- D. (config-router-af-topology)#no redistribute ospf 10 match external 1 external 2 metric 1000000 10 255 1 1500

**Answer: B**

## Question 41

Refer to the exhibit.

Lo0: 192.168.1.55  
255.255.255.128



Admin PC

ip address:  
192.168.1.200  
255.255.255.128

```
aaa new-model
!
aaa authentication login default line enable
aaa authorization commands 15 default local
!
!
username admin privilege 15 password cisco123!
!
ip ssh version 2
!
access-list 101 permit tcp 152.162.1.0 0.0.0.255 any eq 22
access-list 101 permit tcp 192.168.5.0 0.0.0.255 any range 22 smtp
!
line vty 0 4
access-class 101 in
password cisco
transport input all
login local
```

An engineer configured user login based on authentication database on the router, but no one can log into the router. Which configuration resolves the issue?

- A. aaa authentication login default enable
- B. aaa authorization network default local
- C. aaa authentication login default local
- D. aaa authorization exec default local

**Answer: C**

#### Question 42

An engineer configures PBR on R5 and wants to create a policy that matches traffic destined toward 10.10.10.0/24 and forwards it toward 10.1.1.1. This traffic must also have its IP precedence set to 5. All other traffic should be forwarded toward 10.1.1.2 and have its IP precedence set to 0. Which configuration meets the requirements?

Option A

```
access-list 1 permit 10.10.10.0 0.0.0.255
route-map CCNP permit 10
match ip address 1
set ip next-hop 10.1.1.1
set ip precedence 5
!
route-map CCNP permit 20
set ip next-hop 10.1.1.2
set ip precedence 0
```

Option B

	<pre> access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10   match ip address 100   set ip next-hop 10.1.1.1   set ip precedence 0 ! route-map CCNP permit 20   set ip next-hop 10.1.1.2   set ip precedence 5 ! route-map CCNP permit 30 </pre>
<p>Option C</p> <pre> access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10   match ip address 100   set ip next-hop 10.1.1.1   set ip precedence 5 ! route-map CCNP permit 20   set ip next-hop 10.1.1.2   set ip precedence 0 </pre>	<p>Option D</p> <pre> access-list 1 permit 10.10.10.0 0.0.0.255 access-list 2 permit any route-map CCNP permit 10   match ip address 1   set ip next-hop 10.1.1.1   set ip precedence 5 ! route-map CCNP permit 20   match ip address 2   set ip next-hop 10.1.1.2   set ip precedence 0 ! route-map CCNP permit 30 </pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

### Question 43

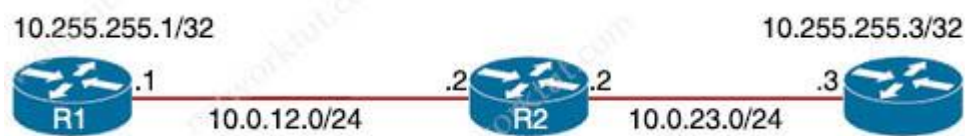
An engineer received a ticket about a router that has reloaded. The monitoring system graphs show different traffic patterns between logical and physical interfaces when the router is rebooted. Which action resolves the issue?

- A. Configure the snmp ifindex persist command globally.
- B. Clear the logical interfaces with snmp ifindex clear command
- C. Configure the snmp ifindex persist command on the physical interfaces.
- D. Trigger a new snmpwalk from the monitoring system to synchronize interface OIDs

**Answer: A**

### Question 44

Refer to the exhibit.



```
PE1# show run | sec router bgp
router bgp 65000
  bgp log-neighbor-changes
  neighbor 10.255.255.3 remote-as 65000
  neighbor 10.255.255.3 update-source Loopback0
PE1# debug ip tcp transactions
PE1# debug ip icmp
[...snip...]

*Feb 22 14:04:12.374: TCP: sending SYN, seq 379810712, ack 0
*Feb 22 14:04:12.374: TCP0: Connection to 10.255.255.3:179,
advertising MSS 1460
*Feb 22 14:04:12.374: TCP0: state was CLOSED -> SYNSENT [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: ICMP: dst (10.255.255.1) administratively
prohibited unreachable rcv from 10.0.12.2
*Feb 22 14:04:12.375: TCP0: ICMP destination unreachable received
*Feb 22 14:04:12.375: Released port 21381 in Transport Port
Agent for TCP IP type 1 delay 240000
*Feb 22 14:04:12.375: TCP0: state was SYNSENT -> CLOSED [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: TCB 0xE35A92B8 destroyed
```

The administrator is troubleshooting a BGP peering between PE1 and PE3 that is unable to establish. Which action resolves the issue?

- A. P2 must have a route to PE3 to establish a BGP session to PE1
- B. Disable sending ICMP unreachables on P2 to allow PE1 to establish a session with PE3
- C. Ensure that the PE3 loopback address is used as a source for BGP peering to PE1
- D. Remove the traffic filtering rules on P2 blocking the BGP communication between PE1 and PE3

**Answer: C**

### Question 45

Refer to the exhibits.

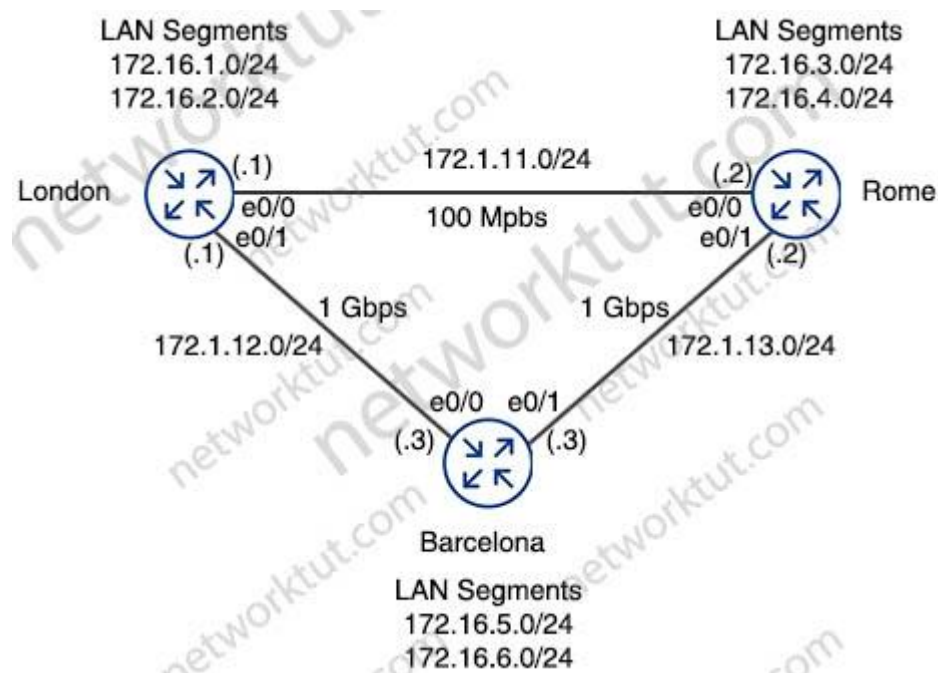
London - "show ip route" output  
Gateway of last resort is not set

172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks  
 C 172.1.11.0/24 is directly connected, Ethernet0/0  
 L 172.1.11.1/32 is directly connected, Ethernet0/0  
 C 172.1.12.0/24 is directly connected, Ethernet0/1  
 L 172.1.12.1/32 is directly connected, Ethernet0/1  
 D 172.1.13.0/24 [90/76800] via 172.1.11.2, 00:00:50, Ethernet0/0  
 172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks  
 C 172.16.1.0/24 is directly connected, Loopback0  
 L 172.16.1.1/32 is directly connected, Ethernet0/0  
 C 172.16.2.0/24 is directly connected, Loopback1  
 L 172.16.2.1/32 is directly connected, Loopback1  
 R 172.16.3.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0  
 R 172.16.4.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0  
 D 172.16.5.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1  
 D 172.16.6.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1

Rome - "show run | section router" output

```

router eigrp 111
 network 172.1.0.0
 network 172.16.0.0
 no auto-summary
  
```



London must reach Rome using a faster path via EIGRP if all the links are up but it failed to take this path. Which action resolves the issue?

- A. Increase the bandwidth of the link between London and Barcelona
- B. Use the network statement on London to inject the 172.16.X.0/24 networks into EIGRP
- C. Change the administrative distance of RIP to 150
- D. Use the network statement on Rome to inject the 172.16.X.0/24 networks into EIGRP

**Answer: D**

### Question 46

Refer to the exhibit.

```
enable secret 5 <password>
username cisco privilege 15 secret 5 <password>
username operator password 7 <password>
line vty 0 4
session-timeout 240
password 7 <password>
transport input telnet
```

The authentication is not working as desired and the user drops into user-exec mode. Which configuration resolves the issue?

<p>Option A</p> <pre>aaa new-model aaa authentication login default local aaa authorization exec default local ! line vty 0 4 login authentication default authorization exec default</pre>	<p>Option B</p> <pre>aaa new-model aaa authentication login default local aaa authorization priv default 15 ! line vty 0 4 login authentication default authorization exec priv15</pre>
<p>Option C</p> <pre>aaa new-model aaa authentication login local aaa authorization exec local ! line vty 0 4 login authentication local authorization exec default</pre>	<p>Option D</p> <pre>aaa new-model aaa authentication common-id default aaa authorization exec default local ! line vty 0 4 login authentication default authorization exec default</pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

### Question 47

Refer to the exhibit.



Dallas\_Router:

```
interface GigabitEthernet0/0/0.364
description Guest_Wifi_10.66.46.0/23
encapsulation dot1Q 364
ip address 10.66.46.1 255.255.254.0
ip helper-address 10.192.104.212
ip helper-address 10.191.103.140
ip access-group GUEST-ACCESS in
ip access-group GUEST-ACCESS-OUT out
no ip redirects
no ip unreachable
no ip proxy-arp

ip access-list extended GUEST-ACCESS
remark Internet Access Only
permit udp any any eq bootpc
permit udp any any eq bootps
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.255.255.255
deny ip any 192.168.0.0 0.255.255.255
deny ip any 224.0.0.0 0.255.255.255
deny ip any 169.254.0.0 0.255.255.255
deny ip any 127.0.0.0 0.255.255.255
deny ip any 192.0.2.0 0.0.0.255
deny ip any host 0.0.0.0
permit ip 10.66.42.0 0.0.0.255 any
permit ip 10.66.46.0 0.0.0.255 any
!

ip access-list extended GUEST-ACCESS-OUT
remark Used to block inbound traffic to Guest Networks
permit udp any any eq bootps
permit udp any any eq bootpc
permit udp any any eq domain
permit udp any any
permit icmp any any
permit tcp host 10.192.103.124 eq 15871 any
permit tcp any any established
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.255.255.255
deny ip any 192.168.0.0 0.255.255.255
deny ip any 224.0.0.0 0.255.255.255
deny ip any 169.254.0.0 0.255.255.255
deny ip any 127.0.0.0 0.255.255.255
deny ip any 192.0.2.0 0.0.0.255
deny ip any host 0.0.0.0
```

After a new regional office is set up, not all guests can access the internet via guest Wi-Fi. Clients are getting the correct IP address from guest Wi-Fi VLAN 364. Which action resolves the issue?

- A. Allow 10.66.46.0/23 in the outbound ACL
- B. Allow DNS traffic through the outbound ACL

- C. Allow DNS traffic through the inbound ACL
- D. Allow 10.66.46.0/23 in the inbound ACL

**Answer: C**

### Question 48

The network administrator configured CoPP so that all routing protocol traffic toward the router CPU is limited to 1 mbps. All traffic that exceeds this limit must be dropped. The router is running BGP and OSPF Management traffic for Telnet and SSH must be limited to 500kbps.

```
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range 22 23
access-list 100 permit ospf any any
!
class-map CM-ROUTING
match access-group 100
class-map CM-MGMT
match access-group 100
!
policy-map PM-COPP
class CM-ROUTING
police 1000000 conform-action transmit
class CM-MGMT
police 500000 conform-action transmit
!
control-plane
service-policy output PM-COPP
```

No traffic is filtering through CoPP, which is resulting in high CPU utilization, which configuration resolves the issue ?

- A. no access-list 100  
access-list 100 permit tcp any any eq 179  
access-list 100 permit ospf any any  
access-list 101 permit tcp any any range 22 23  
!  
class-map CM-MGMT  
no match access-group 100  
match access-group 101
- B. control-plane  
no service-policy output PM-COPP  
service-policy input PM-COPP

C. no access-list 100  
access-list 100 permit tcp any any eq 179  
access-list 100 permit tcp any any range eq 22  
access-list 100 permit tcp any any range eq 23  
access-list 100 permit ospf any any

D. no access-list 100  
access-list 100 permit tcp any any eq 179  
access-list 100 permit ospf any any  
access-list 101 Permit tcp any any range 22 23  
!  
class-map CM-MGMT  
no match access-group 100

**Answer: B**

#### **Question 49**

An engineer is creating a policy that overrides normal routing behavior. If the route to a destination of 10.100.100.0/24 is withdrawn from the routing table, the policy must direct traffic to a next hop of 10.1 1.1. If the route is present in the routing table, then normal forwarding must occur. Which configuration meets the requirements?

A. access-list 100 permit ip any any  
!  
route-map POLICY permit 10  
match ip address 100  
set ip next-hop recursive 10.1.1.1

B. access-list 100 permit ip any 10.100.100.0 0.0.0.255  
!  
Route-map POLICY permit 10  
match ip address 100  
  
set ip default next-hop 10.1.1.1

C. access-list 100 permit ip any 10.100.100.0 0.0.0.255  
!  
route-map POLICY permit 10  
match ip address 100  
set ip next-hop 10.1.1.1  
!  
route map POLICY permit 20

D. access-list 100 permit ip any 10.100.100.0 0.0.0.255  
!  
route map POLICY permit 10  
match ip address 100

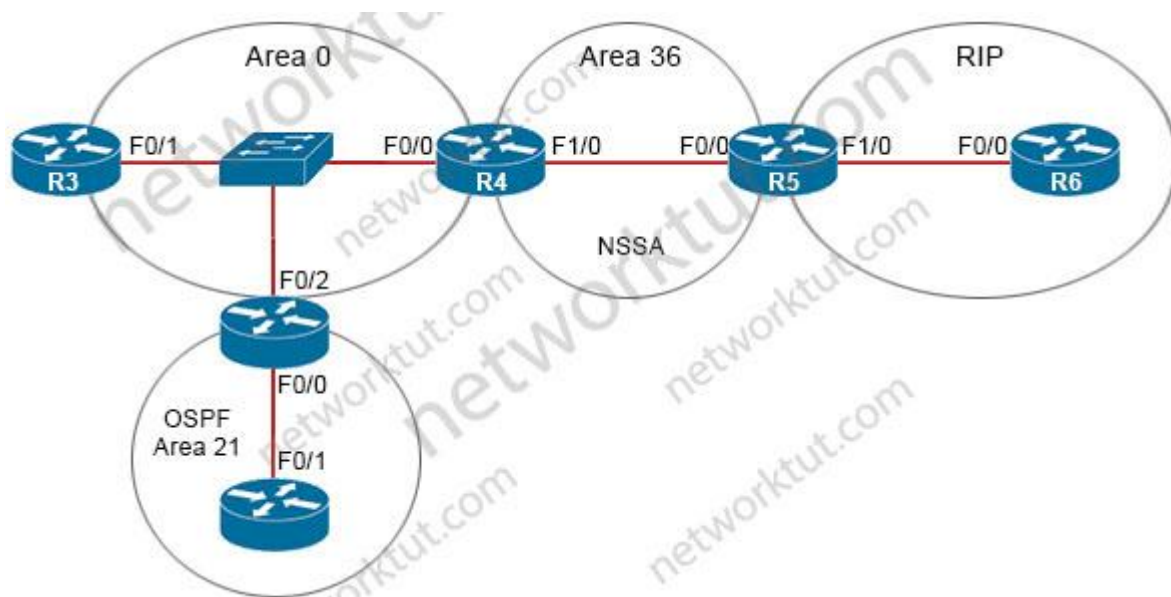
```
set ip next-hop recursive 10.1.1.1
!  
route-map POLICY permit 20
```

**Answer: D**

## New ENARSI Questions 4

### Question 1

Refer to the exhibit.



```
R5# show ip ospf 1 | begin Area 36  
Area 36  
Number of interfaces in this area is 2  
It is a NSSA area  
Area has no authentication  
SPF algorithm last executed 00:32:46.376 ago  
SFF algorithm executed 13 times  
Area ranges are  
172.16.0.0/16 Passive Advertise
```

The network engineer configured the summarization of the RIP routes into the OSPF domain on R5 but still sees four different 172.16.0.0/24 networks on R4. Which action resolves the issue?

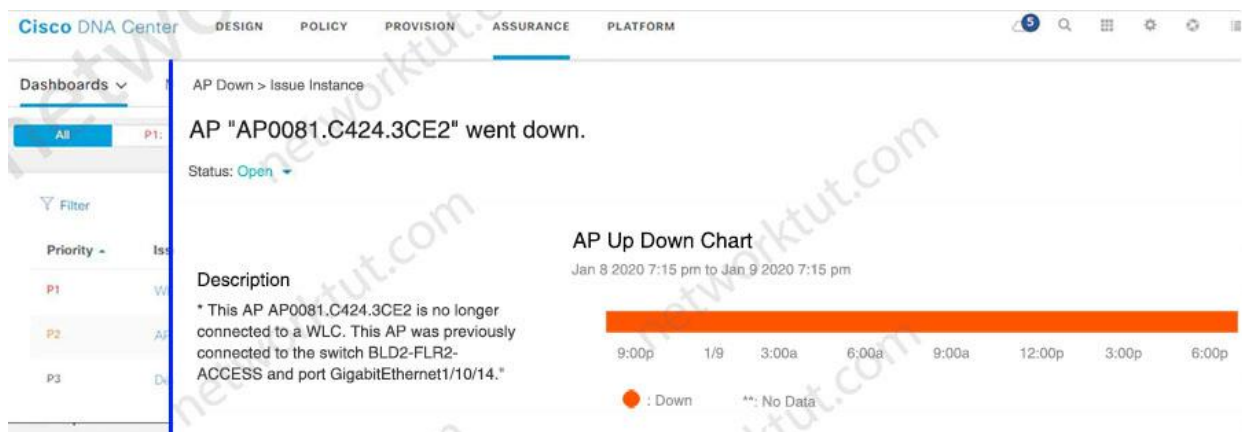
A. R5(config)#router ospf 1  
R5(config-router)#no area  
R5(config-router)#summary-address 172.16.0.0 255.255.252.0

- B. R4(config)#router ospf 99  
 R4(config-router)#network 172.16.0.0 0.255.255.255 area 56  
 R4(config-router)#area 56 range 172.16.0.0 255.255.255.0
- C. R4(config)#router ospf 1  
 R4(config-router)#no area  
 R4(config-router)#summary-address 172.16.0.0 255.255.252.0
- D. R5(config)#router ospf 99  
 R5(config-router)#network 172.16.0.0 0.255.255.255 area 56  
 R5(config-router)#area 56 range 172.16.0.0 255.255.255.0

**Answer: A**

## Question 2

Refer to the exhibit.



The AP status from Cisco DNA Center Assurance Dashboard shows some physical connectivity issues from access switch interface G1/0/14. Which command generates the diagnostic data to resolve the physical connectivity issues?

- A. verify cable-diagnostics tdr interface GigabitEthernet1/0/14
- B. show cable-diagnostics tdr interface GigabitEthernet1/0/14
- C. test cable-diagnostics tdr interface GigabitEthernet1/0/14
- D. check cable-diagnostics tdr interface GigabitEthernet1/0/14

**Answer: C**

## Question 3

Which mechanism provides traffic segmentation within a DMVPN network?

- A. MPLS
- B. BGP
- C. RSVP
- D. IPsec

**Answer: A**

#### **Question 4**

An engineer is implementing a coordinated change with a server team. As part of the change, the engineer must configure interface GigabitEthernet2 in an existing VRF “RED” then move the interface to an existing VRF “BLUE” when the server team is ready. The engineer configured interface GigabitEthernet2 in VRF “RED”:

```
interface GigabitEthernet2
  description Migration ID: B411A21D5032G32
  vrf forwarding RED
  ip address 10.0.0.0 255.255.255.254
  negotiation auto
```

Which configuration completes the change?

A.  
interface GigabitEthernet2  
no ip address  
ip address 10.0.0.0 255.255.255.254  
vrf forwarding BLUE

B.  
interface GigabitEthernet2  
no vrf forwarding RED  
vrf forwarding BLUE  
ip address 10.0.0.0 255.255.255.254

C.  
interface GigabitEthernet2  
no ip address  
vrf forwarding BLUE

D.  
interface GigabitEthernet2  
no vrf forwarding RED  
vrf forwarding BLUE

**Answer: B**

#### **Question 5**

Which function does LDP provide in an MPLS topology?

- A. It exchanges routes for MPLS VPNs across different VRFs.
- B. It enables a MPLS topology to connect multiple VPNs to P routers.
- C. It provides a means for LSRs to exchange IP routes.
- D. It provides hop-by-hop forwarding in an MPLS topology for LSRs.

**Answer: D**

### **Question 6**

An engineer creates a Cisco DNA Center cluster with three nodes, but all the services are running on one host node. Which action resolves this issue?

- A. Click system updates, and upgrade to the latest version of Cisco DNA Center.
- B. Enable service distribution from the Systems 360 page.
- C. Click the master host node with all the services and select services to be moved to other hosts.
- D. Restore the link on the switch interface that is connected to a cluster link on the Cisco DNA Center.

**Answer: B**

### **Question 7**

Which OSI model is used to insert an MPLS label?

- A. between Layer 5 and Layer 6
- B. between Layer 2 and Layer 3
- C. between Layer 3 and Layer 4
- D. between Layer 1 and Layer 2

**Answer: B**

### **Question 8**

The network administrator configured the router for Control Plane Policing to limit OSPF traffic to be policed to 1 Mbps. Any traffic that exceeds this limit must also be allowed at this point for traffic analysis. The router configuration is:

```
access-list 100 permit ospf any any
!
class-map CM-OSPF
  match access-group 100
!
```

```

policy-map PM-COPP
  class CM-OSPF
    police 1000000 conform-action transmit
  !
control-plane
  service-policy output PM-COPP

```

The Control Plane Policing failed to monitor and police OSPF traffic. Which configuration resolves this issue?

<p><b>Option A</b></p> <pre> policy-map PM-COPP class CM-OSPF no police 1000000 conform-action transmit police 1000000 conform-action transmit exceed-action transmit ! control-plane no service-policy output PM-COPP service-policy input PM-COPP </pre>	<p><b>Option B</b></p> <pre> policy-map PM-COPP class CM-OSPF no police 1000000 conform-action transmit police 1000000 conform-action transmit exceed-action transmit </pre>
<p><b>Option C</b></p> <pre> control-plane no service-policy output PM-COPP service-policy input PM-COPP </pre>	<p><b>Option D</b></p> <pre> no access-list 100 access-list 100 deny ospf any any access-list 100 permit ip any any ! policy-map PM-COPP class CM-OSPF no police 1000000 conform-action transmit police 1000000 conform-action transmit exceed-action drop ! control-plane no service-policy output PM-COPP service-policy input PM-COPP </pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

### Question 9

Which feature minimizes DoS attacks on an IPv6 network?



- A. IPv6 Binding Security Table
- B. IPv6 Router Advertisement Guard
- C. IPv6 Prefix Guard
- D. IPv6 Destination Guard

**Answer: D**

### Question 10

The network administrator configured R1 for Control Plane Policing so that the inbound Telnet traffic is policed to 100 kbps. This policy must not apply to traffic coming in from 10.1.1.1/32 and 172.16.1.1/32. The administrator has configured this:

```
access-list 101 permit tcp host 10.1.1.1 any eq 23
access-list 101 permit tcp host 172.16.1.1 any eq 23
!
class-map CoPP-TELNET
  match access-group 101
!
policy-map PM-CoPP
  class CoPP-TELNET
    police 100000 conform transmit exceed drop
!
control-plane
  service-policy input PM-CoPP
```

The network administrator is not getting the desired results. Which set of configurations resolves this issue?

- A.  
control-plane  
no service-policy input PM-CoPP  
!  
interface Ethernet 0/0  
service-policy input PM-CoPP
- B.  
control-plane  
no service-policy input PM-CoPP  
service-policy input PM-CoPP
- C.  
no access-list 101  
access-list 101 deny tcp host 10.1.1.1 any eq 23  
access-list 101 deny tcp host 172.16.1.1 any eq 23  
access-list 101 permit ip any any
- D.  
no access-list 101  
access-list 101 deny tcp host 10.1.1.1 any eq 23

```

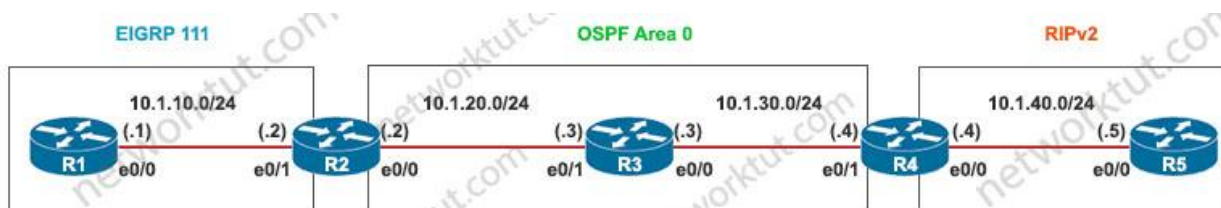
access-list 101 deny tcp host 172.16.1.1 any eq 23
access-list 101 permit ip any any
!
interface E0/0
service-policy input PM-CoPP

```

**Answer: C**

### Question 11

Refer to the exhibit.



```

R2
route-map E20 permit 10
  set tag 111
!
router eigrp 111
 redistribute ospf 1 metric 10 10 10 10 10
!
router ospf 1
 redistribute eigrp 111 route-map E20 subnets

```

```

R4
router rip
 redistribute ospf 1 metric 1
!
router ospf 1
 redistribute rip subnets

```

R5 should not receive any routes originated in the EIGRP domain. Which set of configuration changes removes the EIGRP routes from the R5 routing table to fix the issue?

<b>Option A</b>  R4 route-map O2R deny 10 match tag 111 ! router rip redistribute ospf 1 route-map O2R metric 1	<b>Option B</b>  R4 route-map O2R permit 10 match tag 111 route-map O2R deny 20 ! router rip redistribute ospf 1 route-map O2R metric 1
<b>Option C</b>	<b>Option D</b>

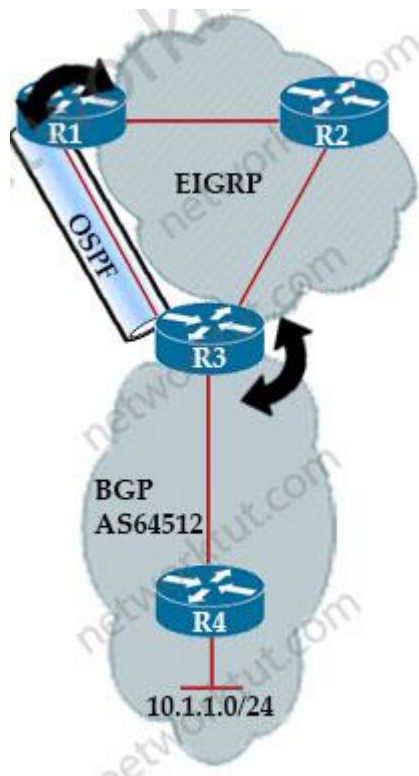
R2 route-map E2O deny 20 R4 route-map O2R deny 10 match tag 111 ! router rip redistribute ospf 1 route-map O2R metric 1	R4 route-map O2R deny 10 match tag 111 route-map O2R permit 20 ! router rip redistribute ospf 1 route-map O2R metric 1
--	--

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

### Question 12

Refer to the exhibit.



BGP and EIGRP are mutually redistributed on R3, and EIGRP and OSPF are mutually redistributed on R1. Users report packet loss and interruption of service to applications hosted on the 10.1.1.0/24 prefix. An engineer tested the link from R3 to R4 with no packet loss present but has noticed frequent routing changes on R3 when running the **debug ip route** command. Which action stabilizes the service?

- A. Tag the 10.1.1.0/24 prefix and deny the prefix from being redistributed into OSPF on R1.
- B. Place an OSPF distribute-list outbound on R3 to block the 10.1.1.0/24 prefix from being advertised back to R3.
- C. Reduce frequent OSPF SPF calculations on R3 that cause a high CPU and packet loss on traffic traversing R3.
- D. Repeat the test from R4 using ICMP ping on the local 10.1.1.0/24 prefix, and fix any Layer 2 errors on the host or switch side of the subnet

**Answer: A**

### Question 13

Refer to the exhibit.

```
R1#sh ipv6 access-list GUARD
IPv6 access list GUARD
deny tcp any host 2001:DB8:A:B::10 eq telnet (6 matches) sequence 10
permit tcp host 2001:DB8:A:A::20 host 2001:DB8:A:B:10 eq telnet sequence 20
permit tcp host 2001:DB8:A:A::2 host 2001:DB8:D::1 eq www sequence 30
permit ipv6 2001:DB8:A:A::/64 any (67 matches) sequence 40
```

PC2 is directly connected to R1. A user at PC2 cannot Telnet to 2001:db8:a:b::10. The user can ping 2001:db8:a:b::10 and receive DHCP-related information from the DHCP server. Which action resolves the issue?

- A. Remove sequence 10 and put it back as sequence 25.
- B. Remove sequence 20 and put it back as sequence 45.
- C. Remove sequence 30 and put it back as sequence 5.
- D. Remove sequence 40 and put it back as sequence 15.

**Answer: A**

### Question 14

What are two characteristics of IPv6 Source Guard? (Choose two)

- A. requires IPv6 snooping on Layer 2 access or trunk ports
- B. used in service provider deployments to protect DDoS attacks
- C. requires the user to configure a static binding
- D. requires that validate prefix be enabled
- E. recovers missing binding table entries

**Answer: D E**

### Question 15

R1 and R2 are configured as eBGP neighbors. R1 is in AS100 and R2 is in AS200, R2 is advertising these networks to R1:

172.16.16.0/20  
172.16.3.0/24  
172.16.4.0/24  
192.168.1.0/24  
192.168.2.0/24  
172.16.0.0/16

The network administrator on R1 must improve convergence by blocking all subnets of 172.16.0.0/16 major network with a mask lower than 23 from coming in. Which set of configurations accomplishes the task on R1?

A. ip prefix-list PL-1 deny 172.16.0.0/16 le 23  
ip prefix-list PL-1 permit 0.0.0.0/0 le 32  
!  
router bgp 100  
neighbor 192.168.100.2 remote-as 200  
neighbor 192.168.100.2 prefix-list PL-1 in

B. ip prefix-list PL-1 deny 172.16.0.0/16 ge 23  
ip prefix-list PL-1 permit 0.0.0.0/0 le 32  
!  
router bgp 100  
neighbor 192.168.100.2 remote-as 200  
neighbor 192.168.100.2 prefix-list PL-1 in

C.  
access-list 1 deny 172.16.0.0 0.0.254.255  
access-list 1 permit any  
!  
router bgp 100  
neighbor 192.168.100.2 remote-as 200  
neighbor 192.168.100.2 distribute-list 1 in

D.  
ip prefix-list PL-1 deny 172.16.0.0/16  
ip prefix-list PL-1 permit 0.0.0.0/0  
!  
router bgp 100  
neighbor 192.168.100.2 remote-as 200  
neighbor 192.168.100.2 prefix-list PL-1 in

**Answer: A**

## Question 16

Refer to the exhibit.

```
aaa new-model
aaa group server radius RADIUS-SERVERS
aaa authentication login default group RADIUS-SERVERS local
aaa authentication enable default group RADIUS-SERVERS enable
aaa authorization exec default group RADIUS-SERVERS if-authenticated
aaa authorization network default group RADIUS-SERVERS if-authenticated
aaa accounting send stop-record authentication failure
aaa session-id common
line con 0
logging synchronous
stopbits 1
line vty 0 4
logging synchronous
transport input ssh
```

A network administrator successfully logs in to a switch using SSH from a RADIUS server. When the network administrator uses a console port to access the switch, the RADIUS server returns “**shell:priv-lvl=15**” and the switch asks to enter the **enable** command. When the command is entered, it gets rejected. Which command set is used to troubleshoot and resolve this issue?

A. line con 0

```
aaa authorization console
authorization exec
!
line vty 0 4
transport input ssh
```

B. line con 0

```
aaa authorization console
!
line vty 0 4
authorization exec
```

C. line con 0

```
aaa authorization console
authorization priv15
!
line vty 0 4
transport input ssh
```

D. line con 0

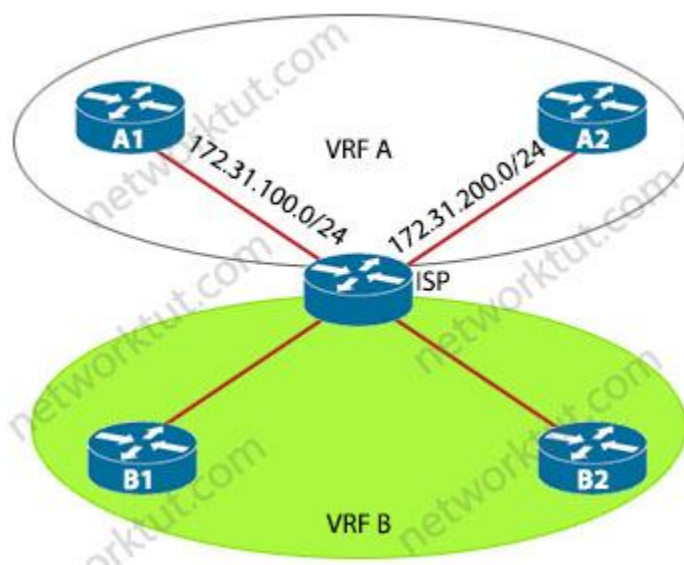
```
aaa authorization console priv15
!
```

```
line vty 0 4
authorization exec
```

**Answer: C**

### Question 17

Refer to the exhibit.



The ISP router is fully configured for customer A and customer B using the VRF-Lite feature. What is the minimum configuration required for customer A to communicate between routers A1 and A2?

Option A	Option B
<pre>A1 interface fa0/0 description To-&gt;ISP ip add 172.31.100.1 255.255.255.0 no shut ! router ospf 100 net 172.31.100.1 0.0.0.255 area 0 A2 interface fa0/0 description To-&gt;ISP ip add 172.31.200.1 255.255.255.0 no shut ! router ospf 100 net 172.31.200.1 0.0.0.255 area 0</pre>	<pre>A1 interface fa0/0 description To-&gt;ISP ip vrf forwarding A ip add 172.31.100.1 255.255.255.0 no shut ! router ospf 100 net 172.31.100.1 0.0.0.255 area 0 A2 interface fa0/0 description To-&gt;ISP ip vrf forwarding A ip add 172.31.200.1 255.255.255.0 no shut !</pre>

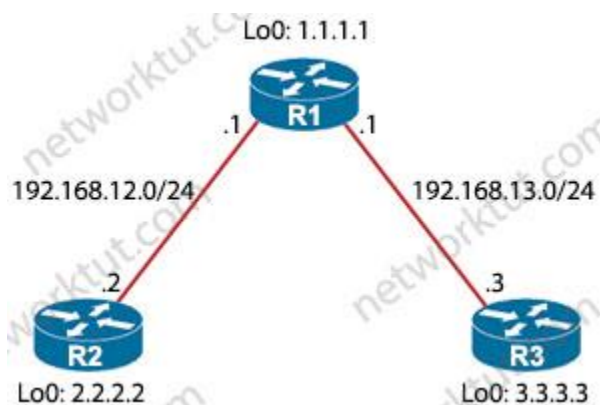
	<pre>router ospf 100 net 172.31.200.1 0.0.0.255 area 0</pre>
<b>Option C</b>  A1 <pre>interface fa0/0 description To-&gt;ISP ip add 172.31.200.1 255.255.255.0 no shut !</pre> <pre>router ospf 100 net 172.31.200.1 0.0.0.255 area 0</pre> A2 <pre>interface fa0/0 description To-&gt;ISP ip add 172.31.100.1 255.255.255.0 no shut !</pre> <pre>router ospf 100 net 172.31.100.1 0.0.0.255 area 0</pre>	<b>Option D</b>  A1 <pre>interface fa0/0 description To-&gt;ISP ip vrf forwarding A ip add 172.31.100.1 255.255.255.0 no shut !</pre> <pre>router ospf 100 vrf A net 172.31.200.1 0.0.0.255 area 0</pre> A2 <pre>interface fa0/0 description To-&gt;ISP ip vrf forwarding A ip add 172.31.100.1 255.255.255.0 no shut !</pre> <pre>router ospf 100 vrf A net 172.31.200.1 0.0.0.255 area 0</pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

### Question 18

Refer to the exhibit.





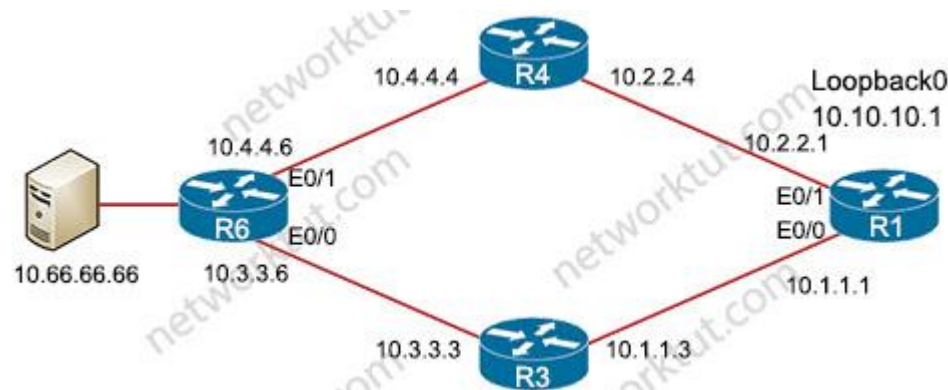
An engineer has configured R1 as EIGRP stub router. After the configuration, router R3 failed to reach to R2 loopback address. Which action advertises R2 loopback back into the R3 routing table?

- A. Use a leak map on R3 that matches the required prefix and apply it with the EIGRP stub feature.
- B. Add a static null route for R2 loopback address in R1 and redistribute it to advertise to R3.
- C. Use a leak map on R1 that matches the required prefix and apply it with the distribute list command toward R3.
- D. Add a static route for R2 loopback address in R1 and redistribute it to advertise to R3.

**Answer: C**

### Question 19

Refer to the exhibit.



```
R6#show ip sla responder
General IP SLA Responder on Control port 1967
General IP SLA Responder on Control V2 port 1167
General IP SLA Responder is: Disabled
```

```
Permanent Port IPSLA Responder
Permanent Port IP SLA Responder is: Disabled
```

```
R6#
interface Ethernet0/0
ip access-group DDOS in
!
interface Ethernet0/1
ip access-group DDOS in

ip access-list extended DDOS
deny icmp any any
permit ip any any
```

```
R1#
track 700 ip sla 700
delay down 30 up 20
!
ip route 10.66.66.0 255 255.255.0 10.2.2.4 track 700
ip route 10.66.66.0 255.255.255.0 10.1.1.3 20
!
ip sla 700
icmp-echo 10.66.66.66 source-ip 10.10.10.1
threshold 100
frequency 5
ip sla schedule 700 life forever start-time now
```

```
R1#show ip sla su
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID    Type Destination Stats Return Last
      (ms) Code Run
-----
*700  icmp-echo 10.66.66.66 - Timeout 9 seconds
ago
```

R1 is configured with IP SLA to check the availability of the server behind R6 but it kept failing. Which configuration resolves the issue?

- A. R6(config)#ip access-list extended DDOS  
R6(config-ext-nacl)#5 permit icmp host 10.10.10.1 host 10.66.66.66
- B. R6(config)#ip sla responder
- C. R6(config)#ip access-list extended DDOS  
R6(config-ext-nacl)#5 permit icmp host 10.66.66.66 host 10.10.10.1
- D. R6(config)#ip sla responder udp-echo ip address 10.10.10.1 port 5000

**Answer: A**

### **Question 20**

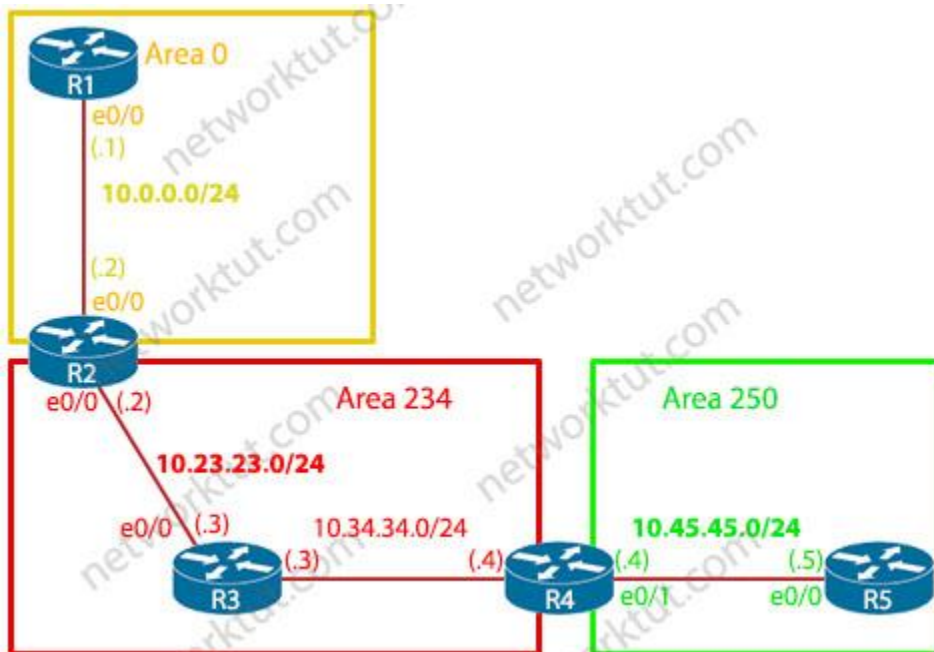
How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?

- A. by MP-BGP
- B. by address family
- C. by RT
- D. by RD

**Answer: D**

### **Question 21**

Refer to the exhibit.



### ABR Configuration:

<b>R2</b> router ospf 1 router-id 0.0.0.22 area 234 virtual-link 10.34.34.4 network 10.0.0.0 0.0.0.255 area 0 network 10.2.2.0 0.0.0.255 area 0 network 10.22.22.0 0.0.0.255 area 234 network 10.23.23.0 0.0.0.255 area 234	<b>R4</b> router ospf 1 router-id 0.0.0.44 area 234 virtual-link 10.23.23.2 network 10.34.34.0 0.0.0.255 area 234 network 10.44.44.0 0.0.0.255 area 234 network 10.45.45.0 0.0.0.255 area 250
--	---

### Virtual Link Status:

```

R2# show ip ospf virtual-links
Run as demand circuit
DoNotAge LSA allowed.
Transit area 234
Topology-MTID    Cost    Disabled    Shutdown    Topology Name
0                65535     no         no         Base
Transmit Delay is 1 sec, State DOWN,

```

The network administrator configured the network to connect two disjointed networks and all the connectivity is up except the virtual link, which causes area 250 to be unreachable. Which two configurations resolve this issue? (Choose two)

A. R2  
router ospf 1  
router-id 10.23.23.2

B. R2  
router ospf 1

```
no area area 234 virtual-link 10.34.34.4
area 0 virtual-link 0.0.0.44
```

C. R4

```
router ospf 1
no area 234 virtual-link 10.23.23.2
area 234 virtual-link 0.0.0.22
```

D. R2

```
router ospf 1
no area 234 virtual-link 10.34.34.4
area 234 virtual-link 0.0.0.44
```

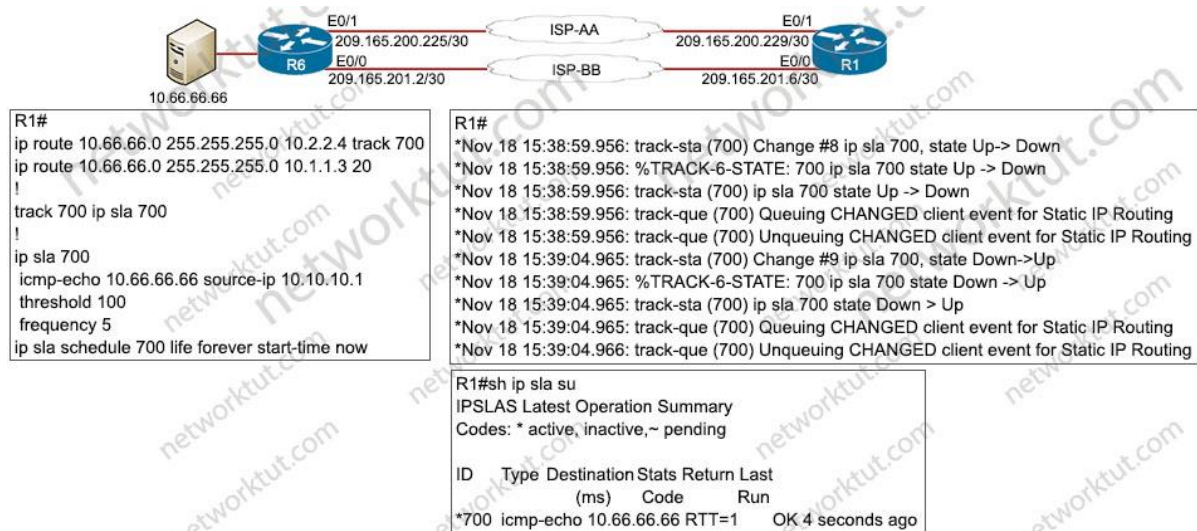
E. R4

```
router ospf 1
no area area 234 virtual-link 10.23.23.2
area 0 virtual-link 0.0.0.22
```

**Answer: C D**

## Question 22

Refer to the exhibit.



An engineer configured IP SLA on R1 to avoid the ISP link flapping problem, but it is not working as designed. IP SLA should wait 30 seconds before switching traffic to a secondary connection and then revert to the primary link after waiting 20 seconds, when the primary link is available and stabilized. Which configuration resolves the issue?

A. R1(config)#ip sla 700

R1(config-ip-sla)#delay down 20 up 30

- B. R1(config)#ip sla 700  
R1(config-ip-sla)#delay down 30 up 20
- C. R1(config)#track 700 ip sla 700  
R1(config-track)#delay down 20 up 30
- D. R1(config)#track 700 ip sla 700  
R1(config-track)#delay down 30 up 20

**Answer: D**

### **Question 23**

A CoPP policy is applied for receiving SSH traffic from the WAN interface on a Cisco ISR4321 router. However, the SSH response from the router is abnormal and stuck during the high link utilization. The problem is identified as SSH traffic does not match in the ACL. Which action resolves the issue?

- A. Rate-limit SSH traffic to ensure dedicated bandwidth.
- B. Apply CoPP on the control plane interface.
- C. Increase the IP precedence value of SSH traffic to 6.
- D. Apply CoPP on the WAN interface inbound direction.

**Answer: B**

### **Question 24**

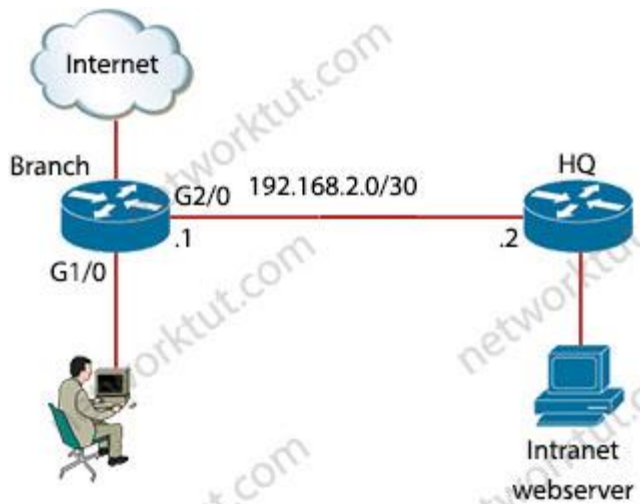
What is a characteristic of Layer 3 MPLS VPNs?

- A. Authentication is performed by using digital certificates or preshared keys.
- B. Engineering capabilities provide QoS and SLAs.
- C. Traffic engineering supports multiple IGP instances.
- D. LSP signaling requires the use of unnumbered IP links for traffic engineering.

**Answer: B**

### **Question 25**

Refer to the exhibit.



The branch router is configured with a default route toward the Internet and has no routes configured for the HQ site that is connected through interface G2/0. The HQ router is fully configured and does not require changes. Which configuration on the branch router makes the intranet website (TCP port 80) available to the branch office users?

#### Option A

```
access-list 100 permit tcp host intranet-
webserver-ip eq 80 any
!
route-map pbr permit 10
match ip address 100
set ip next-hop 192.168.2.2
!
interface G1/0
ip policy route-map pbr
```

#### Option B

```
access-list 101 permit tcp any any eq 80
access-list 102 permit tcp any host intranet-
webserver-ip
!
route-map pbr permit 10
match ip address 101
set ip next-hop 192.168.2.2
route-map pbr permit 20
match ip address 102
set ip next-hop 192.168.2.2
!
interface G2/0
ip policy route-map pbr
```

#### Option C

```
access-list 101 permit tcp any any eq 80
access-list 102 permit tcp any host intranet-
webserver-ip
!
route-map pbr permit 10
match ip address 101 102
set ip next-hop 192.168.2.2
!
interface G1/0
ip policy route-map pbr
```

#### Option D

```
access-list 100 permit tcp any host intranet-
webserver-ip eq 80
!
route-map pbr permit 10
match ip address 100
set ip next-hop 192.168.2.2
!
interface G2/0
ip policy route-map pbr
```

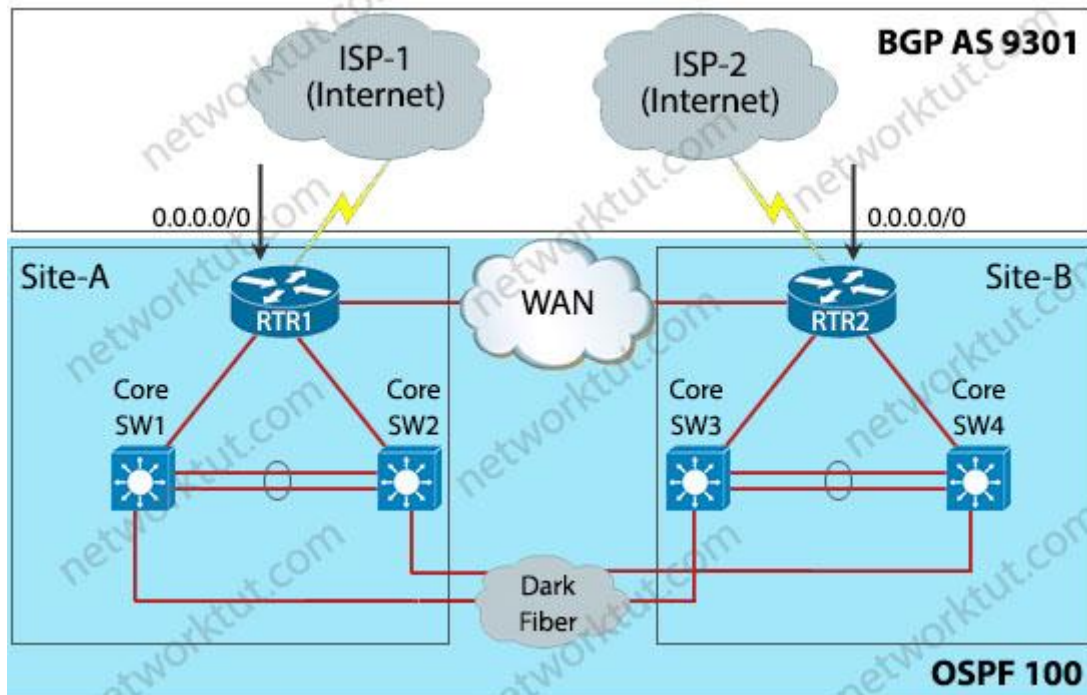
- A. Option A
- B. Option B

- C. Option C
- D. Option D

**Answer: C**

### Question 26

Refer to the exhibit.



The Internet traffic should always prefer Site-A ISP-1 if the link and BGP connection are up; otherwise, all Internet traffic should go to ISP-2. Redistribution is configured between BGP and OSPF routing protocols, and it is not working as expected. What action resolves the issue?

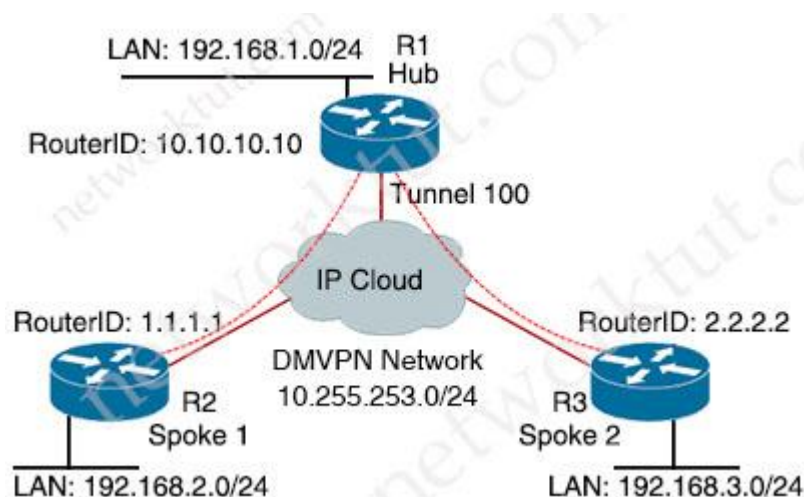
- A. Set OSPF Cost 200 at Site-A RTR1, and set OSPF Cost 100 at Site-B RTR2.
- B. Set metric-type 1 at Site-A RTR1, and set metric-type 2 at Site-B RTR2.
- C. Set metric-type 2 at Site-A RTR1, and set metric-type 1 at Site-B RTR2.
- D. Set OSPF Cost 100 at Site-A RTR1, and set OSPF Cost 200 at Site-B RTR2.

**Answer: B**

### Question 27

Refer to the exhibit.





```

*Mar 1 17:19:04.051: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from
LOADING to FULL, Loading Done
*Mar 1 17:19:06.375: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from FULL
to DOWN, Neighbor Down: Adjacency forced to reset
*Mar 1 17:19:06.627: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from
LOADING to FULL, Loading Done
*Mar 1 17:19:10.123: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from FULL
to DOWN, Neighbor Down: Adjacency forced to reset
*Mar 1 17:19:14.499: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from
LOADING to FULL, Loading Done
*Mar 1 17:19:19.139: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from
EXSTART to DOWN, Neighbor Down: Interface down or detached
*Mar 1 17:01:51.975: %OSPF-4-NONEIGHBOR: Received database description from unknown
neighbor 192.168.1.1
*Mar 1 17:01:57.783: OSPF: Rev LS UPD from 192.168.1.1 on Tunnel100 length 88 LSA count
1
*Mar 1 17:01:57.155: OSPF: Send UPD to 10.255.253.1 on Tunnel100 length 100 LSA count 2

```

A network administrator sets up an OSPF routing protocol for a DMVPN network on the hub router. Which configuration command is required to establish a DMVPN tunnel with multiple spokes?

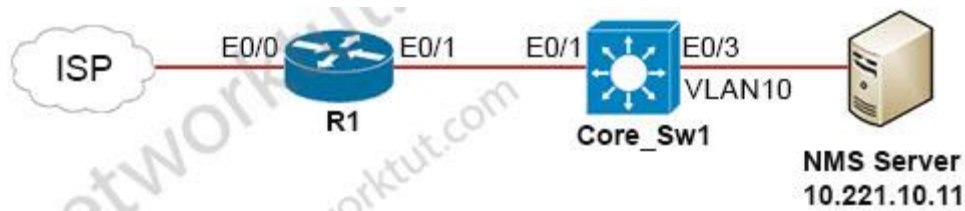
- A. ip ospf network point-to-multipoint on both spoke routers
- B. ip ospf network point-to-point on both spoke routers
- C. ip ospf network point-to-multipoint on one spoke router
- D. ip ospf network point-to-point on the hub router

**Answer: A**

## Question 28

Refer to the exhibit.





```

R1#sh flow exporter
Flow Exporter FlowAnalyzer1:
Description:   User defined
Export protocol: NetFlow Version 9
Transport Configuration:
Destination IP address: 10.221.10.10
Source IP address: 10.2.2.1
Source Interface: Ethernet0/1
Transport Protocol: UDP
Destination Port: 2055
Source Port: 49398
DSCP: 0x0
TTL: 255
Output Features: Not Used
  
```

An engineer configured NetFlow on R1, but the NMS server cannot see the flow from R1. Which configuration resolves the issue?

- A. flow exporter FlowAnalyzer1  
destination 10.221.10.11
- B. interface Ethernet0/0  
flow-destination 10.221.10.11
- C. flow monitor Flowmonitor1  
destination 10.221.10.11
- D. interface Ethernet0/1  
flow-destination 10.221.10.11

**Answer: A**

## Question 29

Refer to the exhibit.

```

*17:40:07.826: AAA/BIND(00000055): Bind i/f
*17:40:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*17:40:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*17:40:07.826: TPLUS(00000055) login timer started 1020 sec timeout
*17:40:07.826: TPLUS: processing authentication start request id 85
*17:40:07.826: TPLUS: Authentication start packet created for 85()
  
```

```
*17:40:07.826: TPLUS: Using server 10.106.60.182
*17:40:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*17:40:07.830: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.830: TPLUS(00000055)/0/READ: Would block while reading
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*17:40:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*17:40:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*17:40:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

An engineer is troubleshooting a TACACS problem. Which action resolves the issue?

- A. Apply a configured AAA profile to the VTY.
- B. Configure a matching TACACS server IP.
- C. Generate authentication from a relative source interface.
- D. Configure a matching preshared key.

**Answer: D**

### **Question 30**

Refer to the exhibit.



A network administrator is troubleshooting IPv6 address assignment for a DHCP client that is not getting an IPv6 address from the server. Which configuration retrieves the client IPv6 address from the DHCP server?

- A. **ipv6 dhcp relay-agent** command on the interface
- B. **ipv6 address autoconfig** command on the interface
- C. **ipv6 dhcp server automatic** command on DHCP server
- D. **service dhcp** command on DHCP server

**Answer: B**

### Question 31

Refer to the exhibit.



```
Switch#  
!  
line con 0  
  logging synchronous  
line aux 0  
line vty 0 4  
  password cisco@123  
  login  
  transport input ssh telnet  
!  
end
```

An engineer must block access to the console ports for all corporate remote Cisco devices based on the recent corporate security policy but the security team still can connect through the console port. Which configuration on the console port resolves the issue?

- A. no exec
- B. transport input telnet
- C. exec 0 0
- D. login and password

**Answer: A**

### Question 32

Refer to the exhibit.

```
R1(config)# ip vrf CCNP  
R1(config-vrf)# rd 1:100  
R1(config-vrf)# exit  
R1(config)# interface Loopback0  
R1(config-if)# ip address 10.1.1.1 255.255.255.0  
R1(config-if)# ip vrf forwarding CCNP  
R1(config-if)# exit  
R1(config)# exit  
R1# ping vrf CCNP 10.1.1.1  
% Unrecognized host or address, or protocol not running.
```

Which command must be configured to make VRF CCNP work?

- A. interface Loopback0  
vrf forwarding CCNP

B. interface Loopback0  
ip address 10.1.1.1 255.255.255.0  
ip vrf forwarding CCNP

C. interface Loopback0  
ip address 10.1.1.1 255.255.255.0  
vrf forwarding CCNP

D. interface Loopback0  
ip address 10.1.1.1 255.255.255.0

**Answer: D**

### Question 33

The network administrator configured R1 to authenticate Telnet connections based on Cisco ISE using TACACS+. ISE has been configured with an IP address of 192.168.1.5 and with a network device pointing toward R1(192.168.1.1) with a shared secret password of Cisco123. The administrator cannot authenticate to R1 based on ISE.

```
aaa new-model
!
tacacs server ISE1
  address ipv4 192.168.1.5
  key Cisco123
!
aaa group server tacacs+ TAC-SERV
  server name ISE1
!
aaa authentication login telnet group TAC-SERV
```

Which configuration fixes the issue?

- A. line vty 0 4  
login authentication telnet
- B. line vty 0 4  
login authentication TAC-SERV
- C. ip tacacs-server host 192.168.1.5 key Cisco123
- D. tacacs-server host 192.168.1.5 key Cisco123

**Answer: A**

### Question 34

A company is expanding business by opening 35 branches over the Internet. A network engineer must configure DMVPN at the branch routers to connect with the hub router and allow NHRP to add spoke routers securely to the multicast NHRP mappings automatically. Which configuration meets this requirement at the hub router?

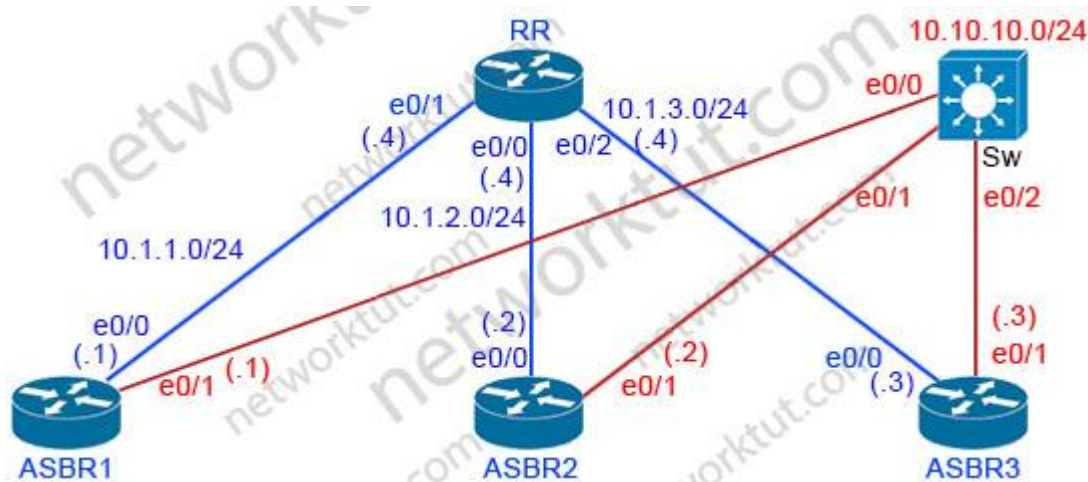
<b>Option A</b>  <pre>interface Tunnel0 ip address 10.0.0.1 255.255.255.0 ip nhrp authentication KEY1 ip nhrp map multicast dynamic ip nhrp network-id 10 tunnel mode gre multipoint</pre>	<b>Option B</b>  <pre>interface Tunnel0 ip address 10.0.0.1 255.255.255.0 ip nhrp authentication KEY1 ip nhrp registration no-unique ip nhrp network-id 10 tunnel mode gre nmba</pre>
<b>Option C</b>  <pre>interface Tunnel0 ip address 10.0.0.1 255.255.255.0 ip nhrp authentication KEY1 ip nhrp map multicast 224.0.0.0 ip nhrp network-id 10 tunnel mode gre ipv4</pre>	<b>Option D</b>  <pre>interface Tunnel0 ip address 10.0.0.1 255.255.255.0 ip nhrp authentication KEY1 ip nhrp nhs dynamic ip nhrp network-id 10 tunnel mode mgre auto</pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

### Question 35

Refer to the exhibit.



<b>RR</b> <pre>router bgp 100 neighbor 10.1.1.1 remote-as 100 neighbor 10.1.2.2 remote-as 100 neighbor 10.1.3.3 remote-as 100</pre>	<b>ASBR2</b> <pre>router bgp 100 neighbor 10.1.1.4 remote-as 100</pre>
--	---

<b>ASBR3</b> router bgp 100 neighbor 10.1.2.4 remote-as 100	<b>ASBR4</b> router bgp 100 neighbor 10.1.3.4 remote-as 100
---	---

The administrator configured the network device for end-to-end reachability, but the ASBRs are not propagation routes to each other. Which set of configuration resolves this issue?

<b>Option A</b>  router bgp 100 neighbor 10.1.1.1 update-source Loopback0 neighbor 10.1.2.2 update-source Loopback0 neighbor 10.1.3.3 update-source Loopback0	<b>Option B</b>  router bgp 100 neighbor 10.1.1.1 ebgp-multihop neighbor 10.1.2.2 ebgp-multihop neighbor 10.1.3.3 ebgp-multihop
<b>Option C</b>  router bgp 100 neighbor 10.1.1.1 route-reflector-client neighbor 10.1.2.2 route-reflector-client neighbor 10.1.3.3 route-reflector-client	<b>Option D</b>  router bgp 100 neighbor 10.1.1.1 next-hop-self neighbor 10.1.2.2 next-hop-self neighbor 10.1.3.3 next-hop-self

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

### Question 36

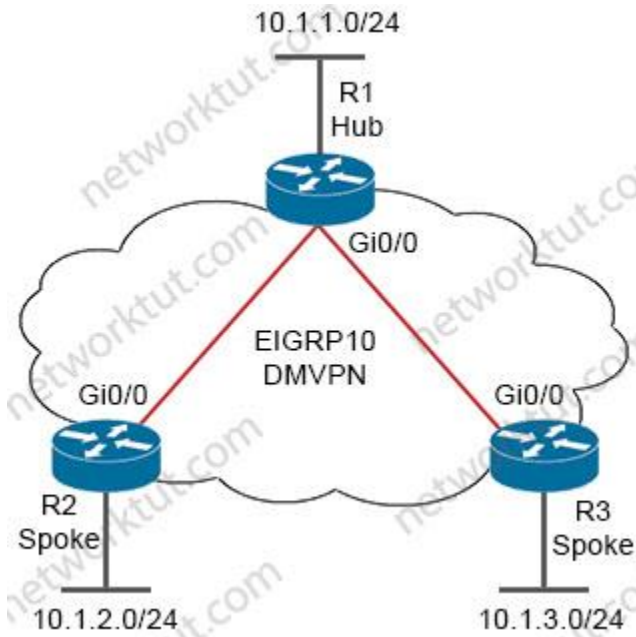
What is a function of IPv6 Source Guard?

- A. It denies traffic from known sources and allocated addresses.
- B. It inspects ND and DHCP packets to build an address binding table.
- C. It works with address glean or ND to find existing addresses.
- D. It notifies the ND protocol to inform hosts if the traffic is denied by it.

**Answer: C**

### Question 37

Refer to the exhibit.



```
R2#show ip route eigrp | include 10.1.
D      10.1.1.0/24
```

```
R3#show ip route eigrp | include 10.1.
D      10.1.1.0/24
```

An engineer configures DMVPN and receives the hub location prefix of 10.1.1.0/24 on R2 and R3. The R3 prefix of 10.1.3.0/24 is not received on R2, and the R2 prefix 10.1.2.0/24 is not received on R3. Which action resolves the issue?

- A. Split horizon prevents the routes from being advertised between spoke routers it should be disabled with the command `no ip split-horizon eigrp 10` on the tunnel interface of R1
- B. There is no spoke-to-spoke connection DMVPN configuration should be modified to enable a tunnel connection between R2 and R3 and neighbor relationship confirmed by use of the `show ip eigrp neighbor` command
- C. Split horizon prevents the routes from being advertised between spoke routers it should be disabled with the `no ip split-horizon eigrp 10` command on the Gi0/0 interface of R1.
- D. There is no spoke-to-spoke connection DMVPN configuration should be modified with a manual neighbor relationship configured between R2 and R3 and confirmed by use of the `show ip eigrp neighbor` command.

**Answer: A**

### Question 38

Refer to the exhibit.

```
R1#show ip interface GigabitEthernet0/0 | include drops
```

```
0 verification drops
0 suppressedverification drops
```



```
R1#show ip interface GigabitEthernet0/1 | include drops
```

```
5 verification drops
0 suppressedverification drops
```

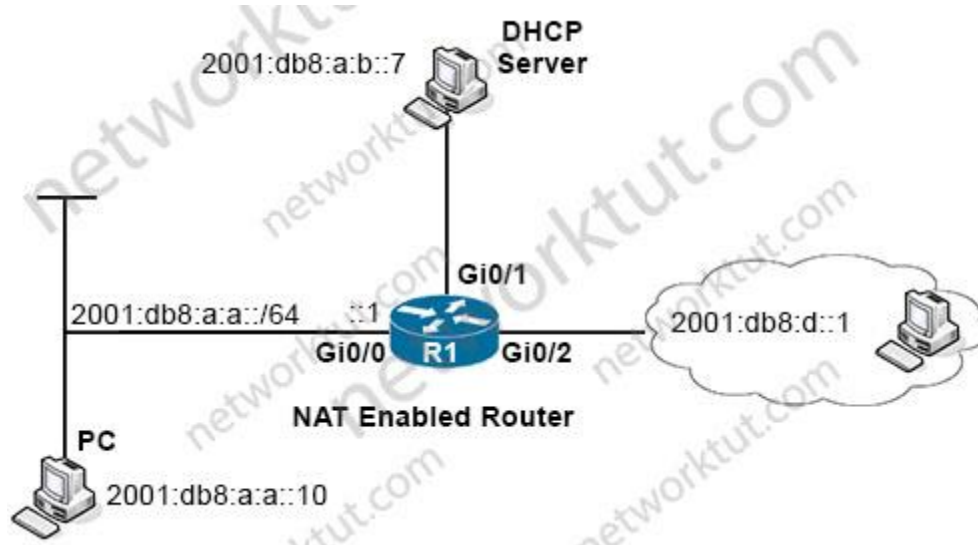
R1 is configured with uRPF, and ping to R1 is failing from a source present in the R1 routing table via the GigabitEthernet 0/0 interface. Which action resolves the issue?

- A. Remove the access list from the interface GigabitEthernet 0/0
- B. Modify the uRPF mode from strict to loose
- C. Enable Cisco Express Forwarding to ensure that uRPF is functioning correctly
- D. Add a floating static route to the source on R1 to the GigabitEthernet 0/1 interface

**Answer: B**

### Question 39

Refer to the exhibit.



```
C:\PC> ping 2001:db8:a:b::7
```

```
Pinging 2001:db8:a:b::7 with 32 bytes of data:
Reply from 2001:db8:a:b::7: time=46ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Ping statistics for 2001:db8:a:b::7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
Minimum = 40ms, Maximum = 46ms, Average = 41ms
```

```
R1# telnet 2001:db8:a:b::7
```

```
Trying 2001:DB8:A:B::7... Open
User Access Verification
Password:
```

```
R1# show ipv6 access-list TSHOOT
```

```
IPv6 access list TSHOOT
```

```
deny tcp any host 2001:DB8:A:B::7 eq telnet (6 matches) sequence 10
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:A:B::7 eq telnet sequence 20
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:D::1 eq www sequence 30
permit ipv6 2001:DB8:A:A::/64 any (67 matches) sequence 40
```

An engineer is troubleshooting a failed Telnet session from PC to the DHCP server. Which action resolves the issue?

- A. Remove sequence 10 to add the PC source IP address and add it back as sequence 10.
- B. Remove sequence 20 and add it back to the IPv6 traffic filter as sequence 5.
- C. Remove sequence 30 and add it back to the IPv6 traffic filter as sequence 5.
- D. Remove sequence 20 for sequence 40 in the access list to allow Telnet.

**Answer: B**

#### **Question 40**

What is an advantage of implementing BFD?

- A. BFD provides millisecond failure detection
- B. BFD provides faster updates for any flapping route
- C. BFD is deployed without the need to run any routing protocol
- D. BFD provides better capabilities to maintain the routing table

**Answer: A**

#### **Question 41**

Refer to the exhibit.

```

RR# show running-config
!
interface Ethernet0/1
no ip address
ipv6 address 2001:DB8:1:12::2/64
ipv6 traffic-filter ACL in
!
ipv6 access-list ACL
sequence 10 permit tcp any any eq 22
sequence 20 permit tcp any eq 22 any
sequence 30 permit tcp any any eq bgp
sequence 40 permit tcp any eq bgp any
sequence 50 permit udp any any eq ntp
sequence 60 permit udp any eq ntp any
sequence 70 permit udp any any eq snmp
sequence 80 deny ipv6 any any log

RR# show ipv6 cef ::/0
::/0
  nexthop 2001:DB8:1:12::1 Ethernet0/1

*Feb 23 00:23:17.211: %IPV6_ACL-6-ACCESSLOGDP: list ACL/80
denied icmpv6 2001:DB8:1:12::1 -> FF02::1:FF00:2 (135/0), 7321
packets

```

After a security audit, the administrator implemented an ACL in the route reflector. The RR became unreachable from any router in the network. Which two actions resolve the issue? (Choose two)

- A. Enable the ND proxy feature on the default gateway.
- B. Configure a link-local address on the Ethernet0/1 interface.
- C. Change the next hop of the default route to the link-local address of the default gateway.
- D. Remove the ACL entry 80.
- E. Permit ICMPv6 neighbor discovery traffic in the ACL.

**Answer:** B E

#### Question 42

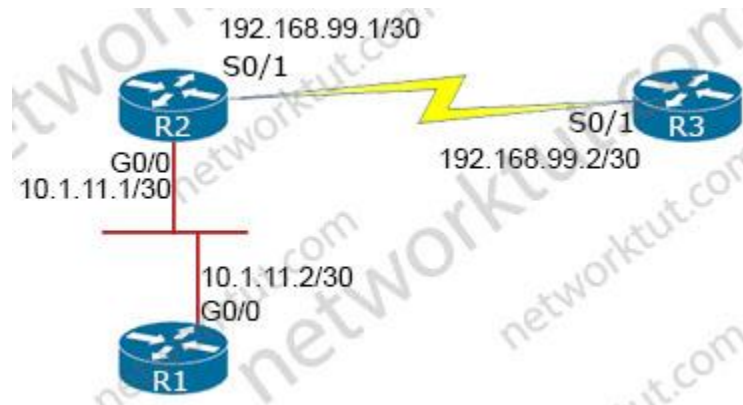
What is the purpose of the DHCPv6 Guard?

- A. It block DHCPv6 messages from relay agents to a DHCPv6 server.
- B. It allows DHCPv6 replay and advertisements from (rouge) DHCPv6 servers.
- C. It messages between a DHCPv6 server and a DHCPv6 client (or relay agent).
- D. It shows that clients of a DHCPv6 server are affected.

**Answer: C**

### Question 43

Refer to the exhibit.



```
R2# show ip ospf neighbor
Neighbor ID    Pri State      Dead Time   Address      Interface
192.168.99.2    1 EXCHANGE/-  00:00:36   192.168.99.1 Serial0/1
router-6#
```

```
R3# show ip ospf neighbor
Neighbor ID    Pri State      Dead Time   Address      Interface
192.168.99.2    1 EXCHANGE/-  00:00:36   192.168.99.2 Serial0/1
```

An OSPF neighbor relationship between R2 and R3 is showing stuck in EXCHANGE/EXSTART state. The neighbor is established between R1 and R2. The network engineer can ping from R2 to R3 and vice versa, but the neighbor is still down. Which action resolves the issue?

- A. Match MTU on both router interfaces or ignore MTU.
- B. Restore the Layer 2/Layer 3 connectivity issue in the ISP network.
- C. Administrative “shut then no shut” both router interfaces.
- D. Enable OSPF on the interface, which is required.

**Answer: A**

### Question 44

Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5

ip sla schedule 1 life forever start-time now
!
```

```
track 1 ip sla 1
!  
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1  
ip route 0.0.0.0 0.0.0.0 198.51.100.1 2 name ISP2
```

The administrator noticed that the connection was flapping between the two ISPs instead of switching to ISP2 when the ISP1 failed. Which action resolves the issue?

- A. Modify the static routes to refer both to the next hop and the outgoing interface.
- B. Reference the track object 1 on the default route through ISP2 instead of ISP1.
- C. Include a valid source-interface keyword in the icmp-echo statement.
- D. Modify the threshold to match the administrative distance of the ISP2 route.

**Answer: C**

### **Question 45**

Refer to the exhibit.

```

Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
Advertised to update-groups:
 1  2  3
(65001 64955 65003) 65089, (Received from a RR-client)
 172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
  Origin IGP, metric 0, localpref 100, valid, confed-internal
  Extended Community: RT:1100:1001
  mpls labels in/out nolaabel/362
(65008 64955 65003) 65089
 172.16.254.226 (metric 20645) from 10.131.123.71 (10.131.123.71)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT:1100:1001
  mpls labels in/out nolaabel/362
(65001 64955 65003) 65089
 172.16.254.226 (metric 20645) from 172.16.216.253 (172.16.216.253)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT:1100:1001
  mpls labels in/out nolaabel/362
(65001 64955 65003) 65089
 172.16.254.226 (metric 20645) from 172.16.216.252 (172.16.216.252)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community: RT:1100:1001
  mpls labels in/out nolaabel/362
(64955 65003) 65089
 172.16.254.226 (metric 20645) from 10.77.255.57 (10.77.255.57)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community RT:1100:1001
  mpls labels in/out nolaabel/362
(64955 65003) 65089
 172.16.254.226 (metric 20645) from 10.57.255.11 (10.57.255.11)
  Origin IGP, metric 0, localpref 100, valid, confed-external, best
  Extended Community RT:1100:1001
  mpls labels in/out nolaabel/362

(64955 65003) 65089
 172.16.254.226 (metric 20645) from 172.16.224.253 (172.16.224.253)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community RT:1100:1001
  mpls labels in/out nolaabel/362
(65003) 65089
 172.16.254.226 (metric 20645) from 172.16.254.234 (172.16.254.234)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community RT:1100:1001
  mpls labels in/out nolaabel/362
65089, (Received from a RR-client)
 172.16.228.226 (metric 20645) from 172.16.228.226 (172.16.228.226)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community RT:1100:1001
  mpls labels in/out nolaabel/278

```

An engineer configured BGP and wants to select the path from 10.77.255.57 as the best path instead of current best path. Which action resolves the issue?



- A. Configure AS\_PATH prepend for the current best path
- B. Configure higher MED to select as the best path
- C. Configure AS\_PATH prepend for the desired best path
- D. Configure lower LOCAL\_PREF to select as the best path

**Answer: D**

#### **Question 46**

Refer to the exhibit.

```
R2(config)# int tun0
*Jun 23 00:42:06.179: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down

R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# tunnel source lo0
R2(config-if)# tunnel destination 10.255.255.1

*Jun 23 00:42:15.845: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to up

R2(config-if)# router eigrp E
R2(config-router)# address-family ipv4 autonomous-system 1
R2(config-router-af)# net 192.168.12.2 0.0.0.0

*Jun 23 00:43:05.730: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.12.1 (Tunnel0) is up: new adjacency
*Jun 23 00:43:05.993: %ADJ-5-PARENT: Midchain parent maintenance
for IP midchain out of Tunnel0 - looped chain attempting to stack
*Jun 23 00:43:15.193: %TUN-5-RECURDOWN: Tunnel0 temporarily
disabled due to recursive routing

*Jun 23 00:43:15.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down
```

An administrator is configuring a GRE tunnel to establish an EIGRP neighbor to a remote router. The other tunnel endpoint is already configured. After applying the configuration as shown, the tunnel started flapping. Which action resolves the issue?

- A. Modify the network command to use the Tunnel0 interface netmask
- B. Advertise the Loopback0 interface from R2 across the tunnel
- C. Stop sending a route matching the tunnel destination across the tunnel
- D. Readdress the IP network on the Tunnel0 on both routers using the /31 netmask

**Answer: C**

#### **Question 47**

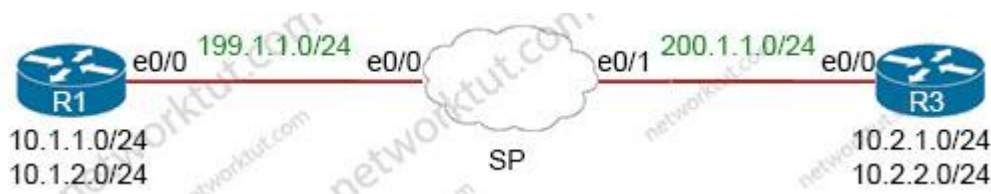
Which two solutions are used to overcome a flapping link that causes a frequent label binding exchange between MPLS routers? (Choose two)

- A. Create link dampening on links to protect the session.
- B. Increase input queue on links to protect the session.
- C. Create targeted hellos to protect the session.
- D. Increase a hold-timer to protect the session.
- E. Increase a session delay to protect the session.

**Answer:** A C

#### Question 48

Refer to the exhibit.



An engineer must configure a LAN-to-LAN IPsec VPN between R1 and the remote router. Which IPsec Phase 1 configuration must the engineer use for the local router?

<p><b>Option A</b></p> <pre>crypto isakmp policy 5 authentication pre-share encryption 3des hash sha group 2 ! crypto isakmp key cisco123 address 200.1.1.3</pre>	<p><b>Option B</b></p> <pre>crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2 ! crypto isakmp key cisco123 address 200.1.1.3</pre>
<p><b>Option C</b></p> <pre>crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2 ! crypto isakmp key cisco123 address 199.1.1.1</pre>	<p><b>Option D</b></p> <pre>crypto isakmp policy 5 authentication pre-share encryption 3des hash md5 group 2 ! crypto isakmp key cisco123! address 199.1.1.1</pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D



**Answer: A**

#### **Question 49**

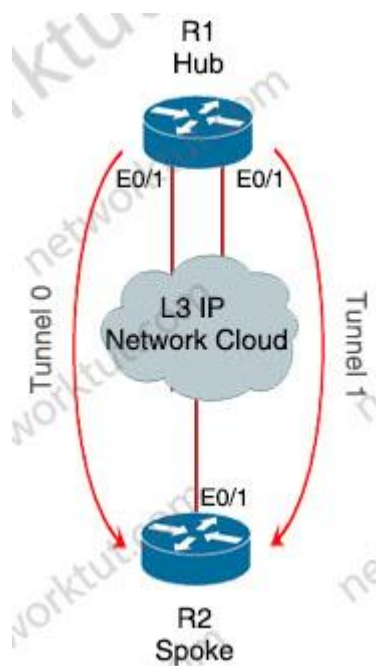
What is a function of an end device configured with DHCPv6 guard?

- A. If it is configured as a server, only prefix assignments are permitted.
- B. If it is configured as a relay agent, only prefix assignments are permitted.
- C. If it is configured as a client, messages are switched regardless of the assigned role.
- D. If it is configured as a client, only DHCP requests are permitted.

**Answer: C**

#### **Question 50**

Refer to the exhibit.



The hub and spokes are configured via two DMVPN tunnel interfaces. The NHRP is configured, and the tunnels are detected on the hub and the spoke. Which configuration command adds an ipsec profile on both tunnel interfaces to encrypt traffic?

- A. Tunnel protection ipsec profile DMVPN unique
- B. Tunnel protection ipsec profile DMVPN tunel1
- C. Tunnel protection ipsec profile DMVPN multipoint
- D. Tunnel protection ipsec profile DMVPN shared

**Answer: D**

### Question 51

What is considered the primary advantage of running BFD?

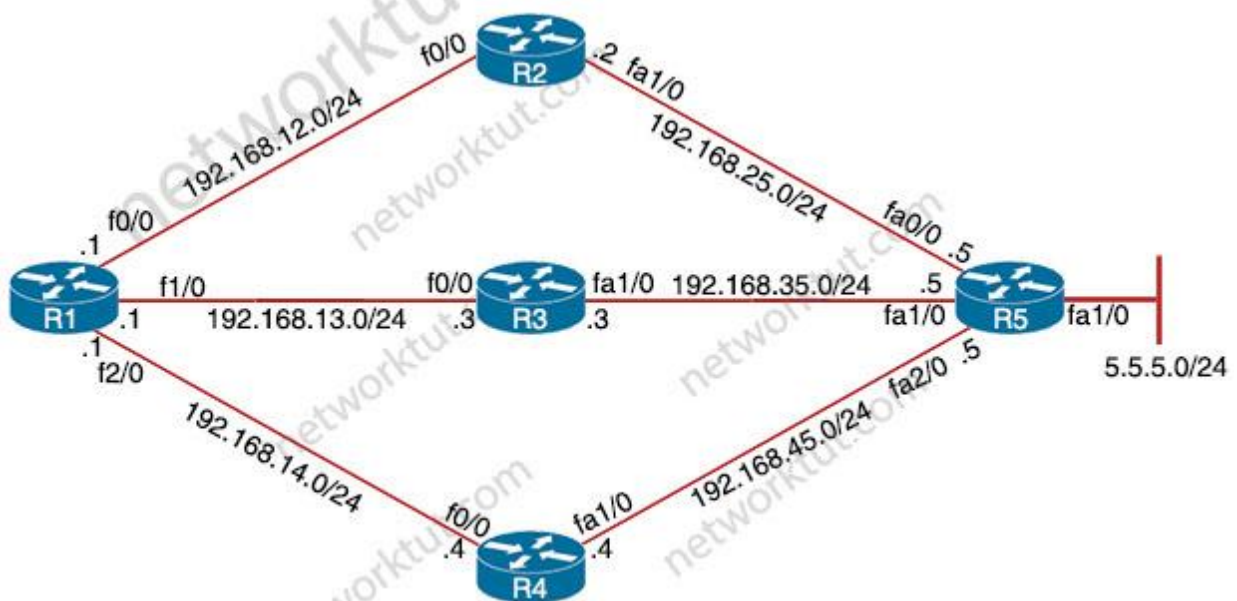
- A. Reduction in CPU needed to detect Layer 2 switch neighbor failures
- B. Reduction in CPU needed to detect Layer 3 switch neighbor failures
- C. Reduction in time needed to detect Layer 2 switch neighbor failures
- D. Reduction in time needed to detect Layer 3 switch neighbor failures

**Answer: D**

### Question 52

Refer to the exhibit.

Known via "eigrp 1", distance 90, metric 158720, type internal  
Redistributing via eigrp 1  
Last update from 192.168.13.3 on Ethernet1/0, 00:00:40 ago  
Routing Descriptor Blocks:  
\* 192.169.13.3, from 192.169.13.3, 00:00:40 ago, via Ethernet1/0  
Route metric is 412160, traffic share count is 23  
Total delay is 6100 microseconds, minimum bandwidth is 10000 Kbit  
Reliability 255/255, minimum MTU 1500 bytes  
Loading 1/255, Hops 2  
192.168.12.2, from 192.169.12.2, 00:00:40 ago, via FasEthernet0/0  
Route metric is 158720, traffic share count is 60  
Total delay is 5200 microseconds, minimum bandwidth is 100000 Kbit  
Reliability 255/255, minimum MTU 1500 bytes  
Loading 1/255, Hops 2



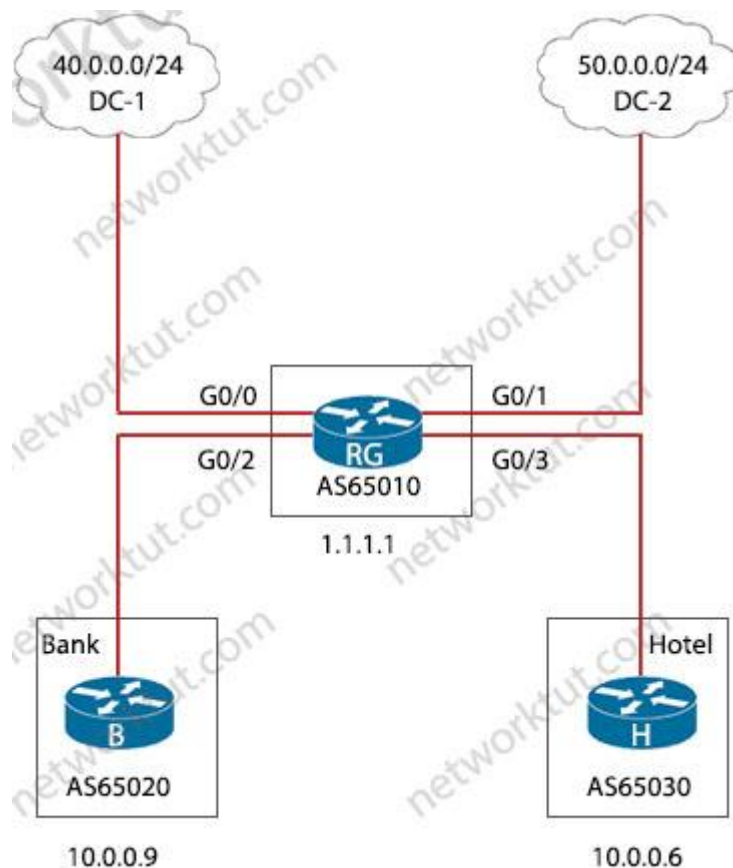
An engineer investigates a routing issue on R1 and finds that traffic destined to 5.5.5.0/24 does not take all of the paths. Which action resolves the issue?

- A. Decrease the variance value in EIGRP.
- B. Increase the variance value in EIGRP.
- C. Remove the adjacency of R3 from EIGRP.
- D. Stop advertising 192.168.13.0/24 in EIGRP.

**Answer: B**

### Question 53

Refer to the exhibit.



Bank users must be restricted to access DC-2 and the Hotel users must be restricted to access DC-1 for respective applications. Interfaces VRF config on RG is:

```
interface GigabitEthernet 0/1
ip vrf forwarding Bank
!
interface GigabitEthernet 0/2
ip vrf forwarding Bank
!
interface GigabitEthernet 0/0
ip vrf forwarding Hotel
```

```
!  
interface GigabitEthernet 0/3  
ip vrf forwarding Hotel
```

Which configuration meets the requirements?

A. Router bgp 65010  
bgp router-id 1.1.1.1  
address-family ipv4 vrf Hotel  
neighbor 10.0.0.6 remote-as 65020  
neighbor 10.0.0.6 activate  
address-family ipv4 vrf Bank  
neighbor 10.0.0.9 remote-as 65030  
neighbor 10.0.0.9 activate

B. Router bgp 65010  
bgp router-id 1.1.1.1  
address-family ipv4 vrf Hotel  
neighbor 10.0.0.9 remote-as 65030  
neighbor 10.0.0.9 activate  
address-family ipv4 vrf Bank  
neighbor 10.0.0.6 remote-as 65020  
neighbor 10.0.0.6 activate

C. Router bgp 65010  
bgp router-id 1.1.1.1  
address-family ipv4 vrf Hotel  
neighbor 10.0.0.9 remote-as 65020  
neighbor 10.0.0.9 activate  
address-family ipv4 vrf Bank  
neighbor 10.0.0.6 remote-as 65030  
neighbor 10.0.0.6 activate

D. Router bgp 65010  
bgp router-id 1.1.1.1  
address-family ipv4 vrf Hotel  
neighbor 10.0.0.6 remote-as 65030  
neighbor 10.0.0.6 activate  
address-family ipv4 vrf Bank  
neighbor 10.0.0.9 remote-as 65020  
neighbor 10.0.0.9 activate

**Answer: D**

### **Question 54**

What are the two prerequisites to enable BFD on Cisco routers? (Choose two)

- A. ICMP must be allowed on all participating routers.
- B. OSPF Demand Circuit must run BFD on all participating routers.
- C. A supported IP routing protocol must be configured on the participating routers.
- D. UDP port 1985 must be allowed on all participating routers.
- E. Cisco Express Forwarding and IP Routing must be enabled on all participating routers.

**Answer: C E**

### Question 55

Refer to the exhibit.

```
R1(config)#ip prefix-list EIGRP seq 10 deny 0.0.0.0/0 le 32
R1(config)#ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
R1(config)#router eigrp 10
R1(config-router)#distribute-list prefix EIGRP in Ethernet0/0
```

A prefix list is created to filter routes inbound to an EIGRP process except for network 10 prefixes. After the prefix list is applied no network 10 prefixes are visible in the routing table from EIGRP. Which configuration resolves the issue?

- A. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9
- B. ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
- C. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9  
ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
- D. ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9  
no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8

**Answer: D**

### Question 56

Refer to the exhibit.

```
R1#sh ip route
      10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D      10.1.2.0/24 [90/409600] via 10.1.100.10, 00:07:33,
FastEthernet0/0
D      10.1.1.0/24 [90/409600] via 10.1.100.10, 00:07:33,
FastEthernet0/0
C      10.1.100.0/24 is directly connected, FastEthernet0/0
```

Although summarization is configured for R1 to receive 10.0.0.0/8, more specific routes are received by R1. How should the 10.0.0.0/8 summary route be received from the neighbor, attached to R1 via Fast Ethernet0/0 interface?

- A. The summarization condition is not met. Router 10.1.100.10 requires a route for 10.0.0.0/8 that points to null 0
- B. R1 should configure the **ip summary-address eigrp <AS number> 10.0.0.0.255.0.0** command under the Fast Ethernet 0/0 interface
- C. The summarization condition is not met. The network 10.1.100.0/24 should be changed to 172.16.0.0/24
- D. R1 should configure the **ip summary-address eigrp <AS number> 10.0.0.0 0.0.0.255** command under the Fast Ethernet 0/0 interface

**Answer: B**

### Question 57

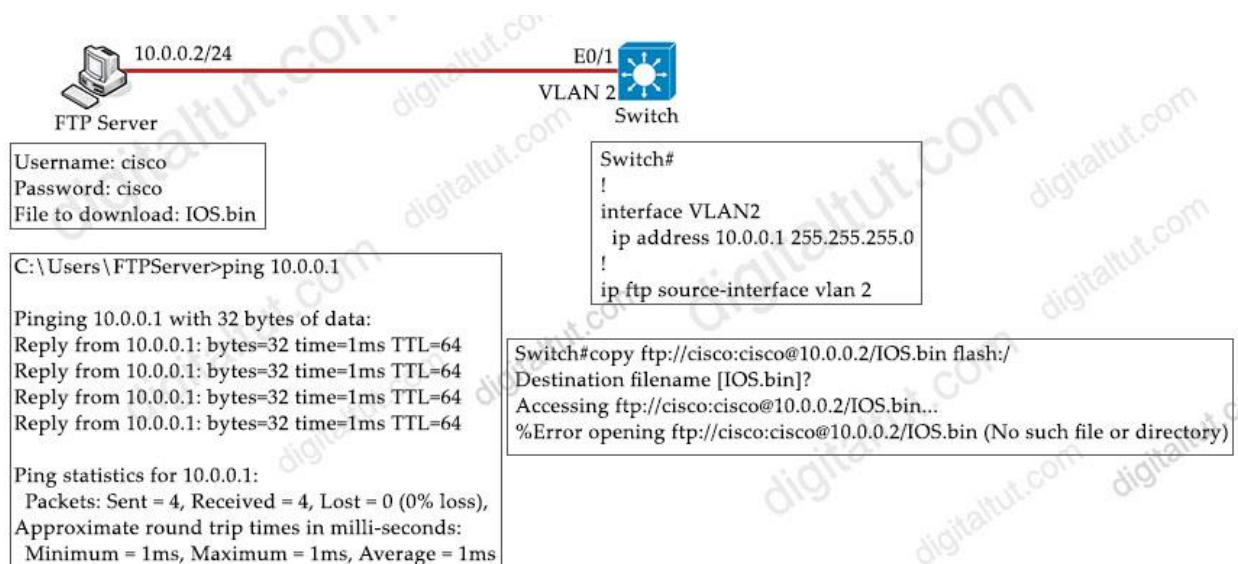
What does the MP-BGP OPEN message contain?

- A. NLRI, path attributes, and IP addresses of the sending and receiving routers
- B. MPLS labels and the IP address of the router that receives the message
- C. IP routing information and the AS number to which the router belongs
- D. the version number and the AS number to which the router belongs

**Answer: D**

### Question 58

Refer to the exhibit.



An engineer cannot copy the IOS.bin. Which action resolves the issue?

- A. Allow file permissions to download the file from the FTP server.
- B. Use the copy flash:/ ftp://cisco@10.0.0.2/IOS.bin command.

- C. Make memory space on the switch flash or USB drive to download the file.
- D. Add the IOS.bin file, which does not exist on FTP server.

**Answer: D**

### Question 59

Refer to the exhibit.

```
Tunnel source 199.1.1.1, destination 200.1.1.3
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

An engineer must establish a point-to-point GRE VPN between R1 and the remote site. Which configuration accomplishes the task for the remote site?

- A. interface Tunnel1  
tunnel source 199.1.1.1  
tunnel destination 200.1.1.3  
ip address 192.168.1.3 255.255.255.0
- B. interface Tunnel1  
tunnel source 200.1.1.3  
tunnel destination 199.1.1.1  
ip address 192.168.1.1 255.255.255.0
- C. interface Tunnel1  
tunnel source 200.1.1.3  
tunnel destination 199.1.1.1  
ip address 192.168.1.3 255.255.255.0
- D. interface Tunnel  
tunnel source 199.1.1.1  
tunnel destination 200.1.1.3  
ip address 192.168.1.1 255.255.255.0

**Answer: C**

===== New Questions (added on 2nd-Mar-2022)  
=====

### Question 60

Refer to the exhibit.

```
ipv6 dhcp pool DHCPPOOL
address prefix 2001:0:1:4::/64 lifetime infinite infinite
```

```
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.240
duplex auto
speed auto
ipv6 address 2001:0:1:4::1/64
ipv6 enable
ipv6 nd ra suppress
ipv6 ospf 1 area 1
ipv6 dhcp server DHCPPOOL
```

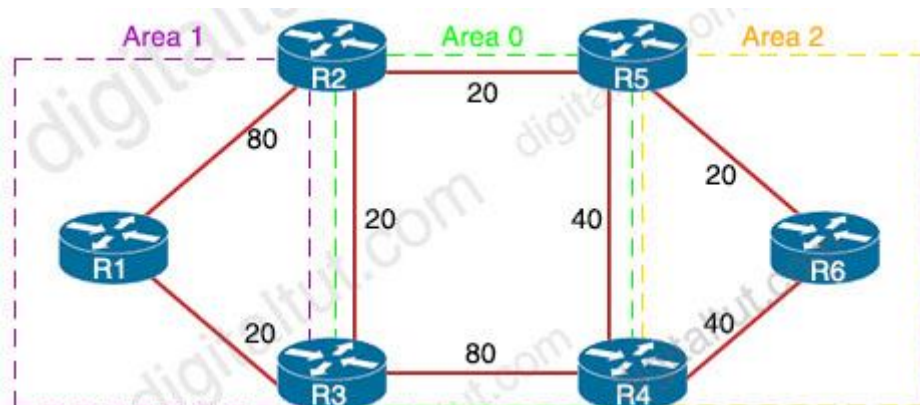
Reachability between servers in a network deployed with DHCPv6 is unstable. Which command must be removed from the configuration to make DHCPv6 function?

- A. ipv6 address 2001:0:1:4::1/64
- B. ipv6 dhcp server DHCPPOOL
- C. ipv6 nd ra suppress
- D. address prefix 2001:0:1:4::/64 lifetime infinite infinite

**Answer: C**

### Question 61

Refer to the exhibit.



R6 should reach R1 via R5>R2>R1. Which action resolves the issue?

- A. Decrease the cost to 2 between R6-R5-R2.
- B. Decrease the cost to 41 between R2 and R1.
- C. Increase the cost to 61 between R2 and R3.
- D. Increase the cost to 61 between R2-R3-R1.



**Answer: C**

### Question 62

Refer to the exhibit.

```
C    10.1.3.0/30 is directly connected, FastEthernet0/1
C    10.1.2.0/30 is directly connected, FastEthernet0/0
C    10.1.1.0/30 is directly connected, FastEthernet1/0
O E2 10.19.0.0/24 [110/20] via 10.1.3.2, 00:02:04, FastEthernet0/1
D    10.55.13.0/24 [90/409600] via 10.1.2.2, 00:01:00, FastEthernet0/0
D    10.37.100.0/24 [90/409600] via 10.1.2.2, 00:01:00, FastEthernet0/0
C    10.100.10.0/29 is directly connected, FastEthernet2/0.10
D    10.55.72.0/24 [90/409600] via 10.1.2.2, 00:01:01, FastEthernet0/0
C    10.100.20.0/29 is directly connected, FastEthernet2/0.20
O E2 10.144.1.0/24 [110/20] via 10.1.3.2, 00:12:51, FastEthernet0/1
D    10.55.144.0/24 [90/409600] via 10.1.2.2, 00:01:01, FastEthernet0/0
O E2 10.123.187.0/24 [110/20] via 10.1.3.2, 00:12:51, FastEthernet0/1
```

#### R2#sh ip eigrp topology

IP-EIGRP Topology Table for AS(100)/ID(10.100.20.2)

Codes: P - Passiver, A - Active, U - Update, Q - Query, R - Reply,  
r - reply Status, s - sia Status

```
P 10.1.3.0/30, 1 successors, FD is 281600 via Connected, FastEthernet0/1
P 10.1.2.0/30, 1 successors, FD is 281600 via Connected, FastEthernet0/0
P 10.1.1.0/30, 1 successors, FD is 28160 via Connected, FastEthernet1/0
P 10.55.13.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.55.100.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.55.72.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.55.144.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.123.187.0/24, 0 successors, FD is inaccessible via 10.1.2.2 (409600/128256), FastEthernet0/0
```

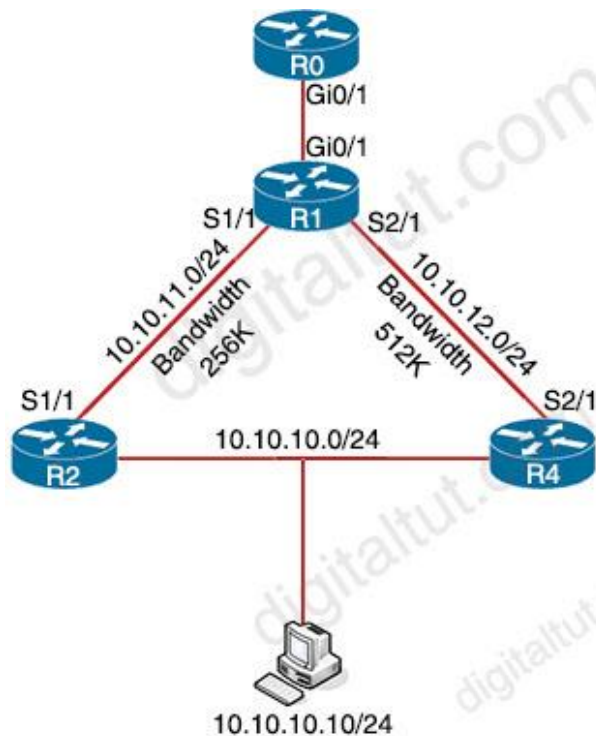
Router R2 should be learning the route for 10.123.187.0/24 via EIGRP. Which action resolves the issue without introducing more issues?

- A. Remove route redistribution in R2 for this route in OSPF.
- B. Use distribute-list to modify the route as an internal EIGRP route.
- C. Redistribute the route in EIGRP with metric, delay, and reliability.
- D. Use distribute-list to filter the external routes in OSPF.

**Answer: A**

### Question 63

Refer to the exhibit.



```

R1#config t
R1(config)#ip access-list extended UDP-ACL
R1(config-ext-nacl)#permit udp any any
R1(config-ext-nacl)#exit
R1(config)#route-map VIA-R2 permit 10
R1(config-route-map)#match ip address UDP-ACL
R1(config-route-map)#set ip next-hop 10.10.11.2
R1(config-route-map)#exit
R1(config)#interface Gi0/1
R1(config-if)#ip policy route-map VIA-R2
R1(config-if)#end
  
```

TCP traffic should be reaching host 10.10.10.10/24 via R2. Which action resolves the issue?

- A. Allow TCP in the access list with no changes to the route map.
- B. Set IP next-hop to 10.10.12.2 under the route-map permit 10 to allow TCP traffic.
- C. Add a permit 20 statement in the route map to allow TCP traffic.
- D. TCP traffic will reach the destination via R2 without any changes.

**Answer: A**

#### Question 64

A customer requested a GRE tunnel through the provider network between two customer sites using loopback to hide internal networks. Which configuration on R2 establishes the tunnel with R1?

```

A. R2(config)#interface Tunnel1
R2(config-if)#ip address 172.20.1.2 255.255.255.0
R2(config-if)#ip mtu 1500
R2(config-if)#ip tcp adjust-mss 1360
R2(config-if)#tunnel source 192.168.20.1
R2(config-if)#tunnel destination 10.10.1.1
  
```

```

B. R2(config)#interface Tunnel1
R2(config-if)#ip address 172.20.1.2 255.255.255.0
R2(config-if)#ip mtu 1400
R2(config-if)#ip tcp adjust-mss 1360
  
```

```
R2(config-if)#tunnel source 192.168.20.1
R2(config-if)#tunnel destination 192.168.10.1
```

```
C. R2(config)#interface Tunnel1
R2(config-if)#ip address 172.20.1.2 255.255.255.0
R2(config-if)#ip mtu 1400
R2(config-if)#ip tcp adjust-mss 1360
R2(config-if)#tunnel source 10.10.2.2
R2(config-if)#tunnel destination 10.10.1.1
```

```
D. R2(config)#interface Tunnel1
R2(config-if)#ip address 172.20.1.2 255.255.255.0
R2(config-if)#ip mtu 1500
R2(config-if)#ip tcp adjust-mss 1360
R2(config-if)#tunnel source 10.10.2.2
R2(config-if)#tunnel destination 10.10.1.1
```

**Answer: C**

### **Question 65**

An engineer failed to run diagnostic commands on devices using Cisco DNA center, which action in Cisco DNA center resolves the issue?

- A. Enable Secure Shell.
- B. Enable Command Runner.
- C. Enable APIs.
- D. Enable CDP.

**Answer: B**

### **Question 66**

Refer to the exhibit.

```
snmp-server community Public RO 90
snmp-server community Private RW 90
R1#show access-list 90
Standard IP access list 90
  permit 10.11.110.11
  permit 10.11.111.12
```

```
Nov 6 06:45:11: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host 10.11.110.12
Nov 6 06:45:12: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host 10.11.110.12
```

A network administrator notices these console messages from host 10.11.110.12 originating from interface E1/0. The administrator considers this an unauthorized attempt to access SNMP on R1. Which action prevents the attempts to reach R1 E1/0?

- A. Configure IOS management plane protection using ACL 90 on interface E1/0.
- B. Configure IOS control plane protection using ACL 90 on interface E1/0.
- C. Add a permit statement including the host 10.11.110.12 into ACL 90.
- D. Create an inbound ACL on interface E1/0 to deny SNMP from host 10.11.110.12.

**Answer: D**

### Question 67

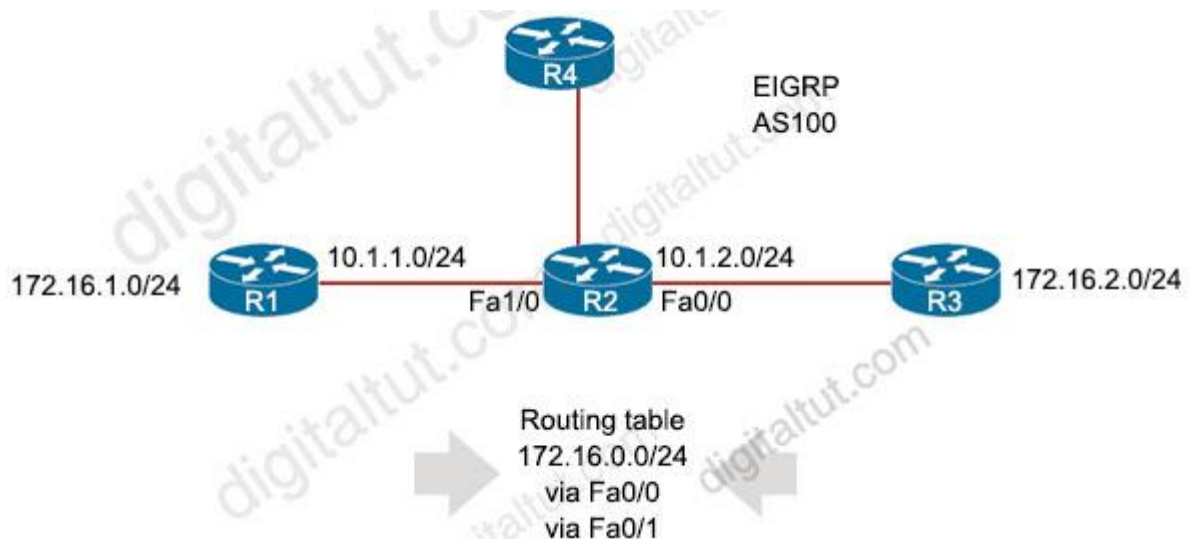
A network administrator added a new spoke site with dynamic IP on the DMVPN network. Which configuration command passes traffic on the DMVPN tunnel from the spoke router?

- A. ip nhrp registration dynamic
- B. ip nhrp registration ignore
- C. ip nhrp registration no-registration
- D. ip nhrp registration no-unique

**Answer: D**

### Question 68

Refer to the exhibit.



R4 is experiencing packet drop when trying to reach 172.16.2.7 behind R2. Which action resolves the issue?

- A. Insert a /24 floating static route on R2 toward R3 with metric 254.
- B. Disable auto summarization on R2.
- C. Insert a /16 floating static route on R2 toward R3 with metric 254.
- D. Enable auto summarization on all three routers R1, R2, and R3.

**Answer: B**

### Question 69

Which two components are required for MPLS Layer 3 VPN configuration? (Choose two)

- A. Use MP-BGP for customer routes.
- B. Use LDP for customer routes.
- C. Use a unique RD per customer VRF.
- D. Use pseudowire for Layer 2 routes.
- E. Use OSPF between PE and CE.

**Answer: A C**

### Question 70

Refer to the exhibit.

```
!- ACL for CoPP Routing class-map
!
access-list 120 permit tcp any gt 1024 eq bgp log
access-list 120 permit tcp any eq bgp gt 1024 established
access-list 120 permit tcp any gt 1024 eq 639
access-list 120 permit tcp any eq 639 gt 1024 established
access-list 120 permit tcp any eq 646
access-list 120 permit udp any eq 646
access-list 120 permit ospf any
access-list 120 permit ospf any host 224.0.0.5
access-list 120 permit ospf any host 224.0.0.6
access-list 120 permit eigrp any
access-list 120 permit eigrp any host 224.0.0.10
access-list 120 permit udp any any eq pim-auto-rp
```

The control plane is heavily impacted after the CoPP configuration is applied to the router. Which command removal lessens the impact on the control plane?

- A. access-list 120 permit eigrp any host 224.0.0.10
- B. access-list 120 permit ospf any
- C. access-list 120 permit udp any any eq pim-auto-rp
- D. access-list 120 permit tcp any gt 1024 eq bgp log

**Answer: D**

### Question 71

Refer to the exhibit.

#### R1 Configuration:

```
key chain cisco
key 2
  key-string abc
!
interface Loopback0
  ip address 10.10.1.1 255.255.255.0
!
interface Serial1/0
  ip address 192.168.10.1 255.255.255.0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 cisco
  serial restart-delay 0
!
router eigrp 100
  network 10.10.1.0 0.0.0.255
  network 192.168.10.0
  no auto-summary
```

#### R2 configuration:

```
key chain cisco
key 1
  key-string 123
key 2
  key-string abc
!
interface Loopback0
  ip address 10.10.2.2 255.255.255.0
!
interface Serial1/0
  ip address 192.168.10.2 255.255.255.0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 cisco
  no fair-queue
!
router eigrp 100
  network 10.10.2.0 0.0.0.255
  network 192.168.10.0
  no auto-summary
```

R1 and R2 are configured for EIGRP peering using authentication and the neighbors failed to come up. Which action resolves the issue?

- A. Configure a matching key-id number on both routers.
- B. Configure a matching lowest key-id on both routers.
- C. Configure a matching key-chain name on both routers.
- D. Configure a matching authentication type on both routers.

**Answer: B**

### Question 72

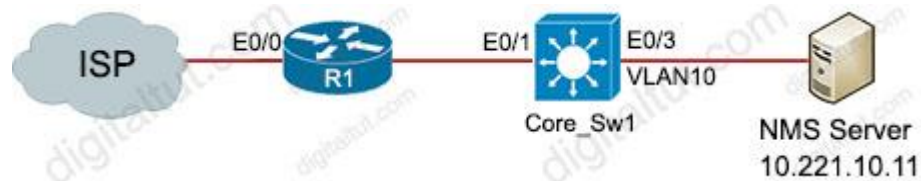
Which method provides failure detection in BFD?

- A. short duration, high overhead
- B. short duration, low overhead
- C. long duration, high overhead
- D. long duration, low overhead

**Answer: B**

### Question 73

Refer to the exhibit.



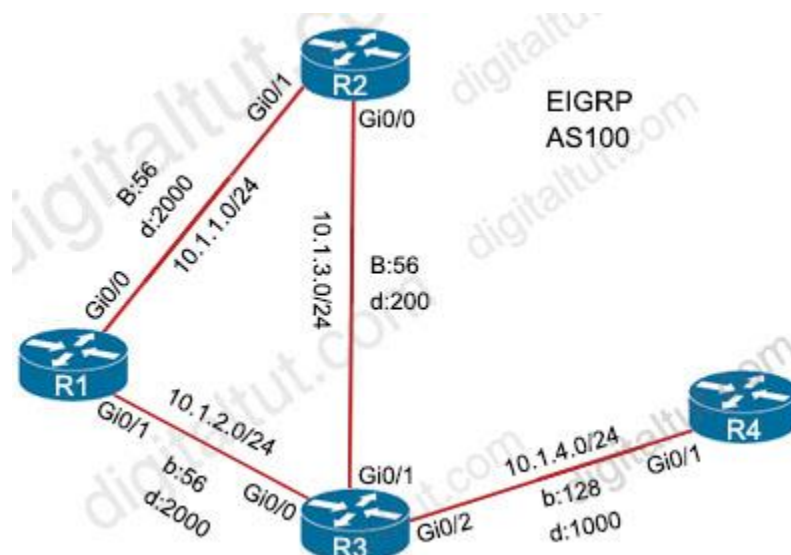
During ISP router maintenance, the network produced many alerts because of the flapping interface. Which configuration on R1 resolves the issue?

- A. snmp trap ip verify drop-rate
- B. no snmp trap link-status
- C. ip verify drop-rate notify hold-down 60
- D. snmp trap link-status down

**Answer: B**

### Question 74

Refer to the exhibit.



A loop occurs between R1, R2, and R3 while EIGRP is run with poison reverse enabled. Which action prevents the loop between R1, R2, and R3?

- A. Configure route tagging.
- B. Enable split horizon.
- C. Configure R3 as stub receive-only.
- D. Configure route filtering.

**Answer: D**

### **Question 75**

A customer reports that traffic is not passing on an EIGRP enabled multipoint interface on a router configured as below:

```
interface Serial0/0/0
  no ip address

interface Serial0/0/0.9 multipoint
  ip address 10.1.1.1 255.255.255.248
  ip split-horizon eigrp 1
```

Which action resolves the issue?

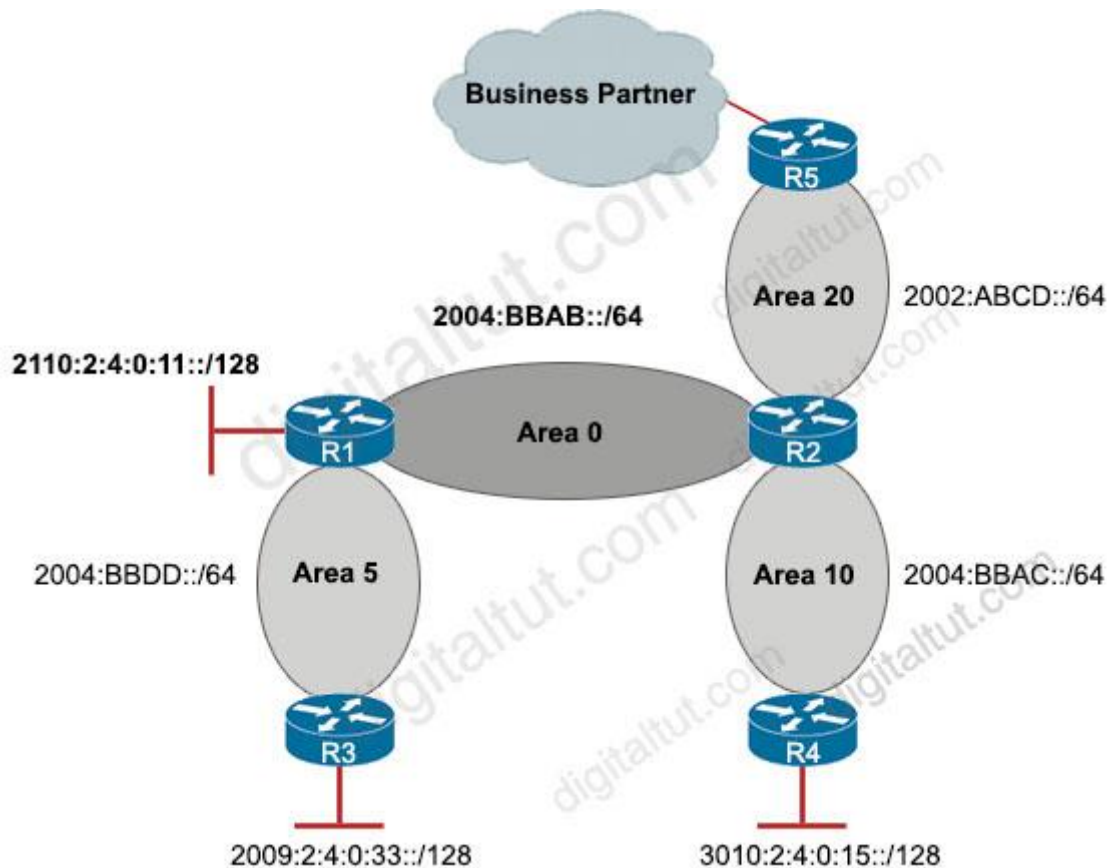
- A. Enable split horizon.
- B. Disable poison reverse.
- C. Disable split horizon.
- D. Enable poison reverse.

**Answer: C**

### **Question 76**

Refer to the exhibit.





```
R2#sh ipv6 route ospf
O 2002:ABCD::/64 [110/1]
  via FastEthernet0/1, directly connected
O 2004:BBAB::/64 [110/1]
  via FastEthernet0/0, directly connected
O 2004:BBAC::/64 [110/1]
  via FastEthernet1/0, directly connected
O 3010:2:4:0:15::/128 [110/1]
  via FE80::C804:1DFF:FB20:8, FastEthernet0/0
```

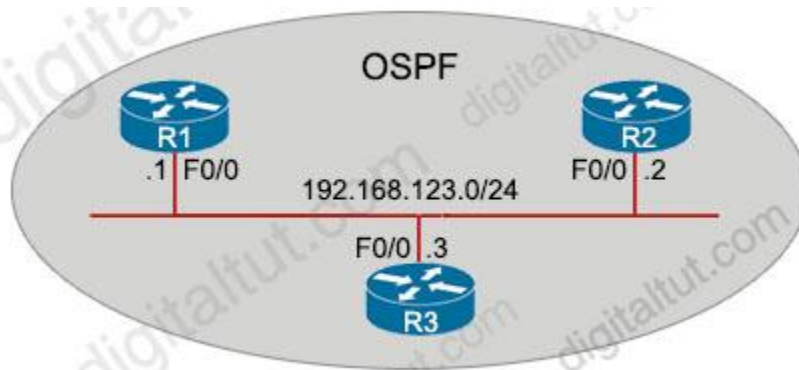
A network engineer applied a filter for LSA traffic on OSPFv3 interarea routes on the area 5 ABR to protect advertising the internal routes of area 5 to the business partner network. All other areas should receive the area 5 internal routes. After the respective route filtering configuration is applied on the ABR, area 5 routes are not visible on any of the areas. How must the filter list be applied on the ABR to resolve this issue?

- A. in the “out” direction for area 20 on router R2
- B. in the “in” direction for area 5 on router R1
- C. in the “out” direction for area 5 on router R1
- D. in the “in” direction for area 20 on router R2

**Answer: A**

**Question 77**

Refer to the exhibit.



**Router R1 Output:**

R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.123.2	1	FULL/BDR	00:00:32	192.168.123.2	FastEthernet0/0
192.168.123.3	1	FULL/DR	00:00:31	192.168.123.3	FastEthernet0/0

**Router R2 Output:**

R2#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.123.1	1	FULL/DROTHER	00:00:32	192.168.123.1	FastEthernet0/0
192.168.123.3	1	FULL/DR	00:00:31	192.168.123.3	FastEthernet0/0

**Router R3 Output:**

R3#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.123.1	1	FULL/DROTHER	00:00:32	192.168.123.1	FastEthernet0/0
192.168.123.2	1	FULL/BDR	00:00:31	192.168.123.2	FastEthernet0/0

An administrator wanted to make R1 always elected as DR, R2 as BDR, and R3 as DROTHER but could not achieve the desired results. Which two configurations resolve the issue? (Choose two)

- A. On the R2 F0/0 interface, configure OSPF priority to 200.
- B. On the R1 F0/0 interface, configure OSPF priority to 202.
- C. On the R2 F0/0 interface, configure OSPF priority to 201.
- D. On the R1 F0/0 interface, configure OSPF priority to 255.
- E. On the R3 F0/0 interface, configure OSPF priority to 201.

**Answer:** C D

**Question 78**

Refer to the exhibit.

```
ip vrf CCNP
 rd 1:1
interface Ethernet1
 ip vrf forwarding CCNP
 ip address 10.1.1.1 255.255.255.252
!
interface Ethernet2
 ip vrf forwarding CCNP
 ip address 10.2.2.2 255.255.255.252
```

Which configuration enables OSPF for area 0 interfaces to establish adjacency with a neighboring router with the same VRF?

A. router ospf 1 vrf CCNP  
network 10.1.1.1 0.0.0.0 area 0  
network 10.2.2.2 0.0.0.0 area 0

B. router ospf 1  
interface Ethernet1  
ip ospf 1 area 0.0.0.0  
interface Ethernet2  
ip ospf 1 area 0.0.0.0

C. router ospf 1 vrf CCNP  
interface Ethernet1  
ip ospf 1 area 0.0.0.0  
interface Ethernet2  
ip ospf 1 area 0.0.0.0

D. router ospf 1 vrf CCNP  
network 10.0.0.0 0.0.255.255 area 0

**Answer: A**

### Question 79

Refer to the exhibit.



An engineer must advertise routes into IPv6 MP-BGP and failed. Which configuration resolves the issue on R1?

A. router bgp 65000  
no bgp default ipv4-unicast  
address-family ipv6 multicast  
network 2001:DB8::/64

B. router bgp 65000  
no bgp default ipv4-unicast  
address-family ipv6 unicast  
network 2001:DB8::/64

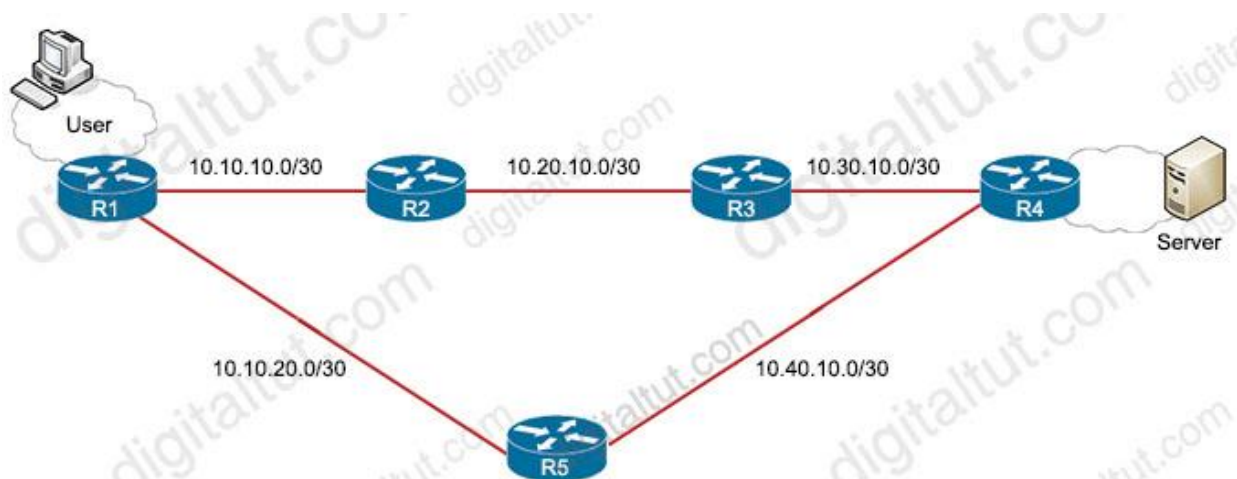
C. router bgp 64900  
no bgp default ipv4-unicast  
address-family ipv6 multicast  
neighbor 2001:DB8:7000::2 translate-update ipv6 multicast

D. router bgp 64900  
no bgp default ipv4-unicast  
address-family ipv6 unicast  
redistribute ospf  
network 2001:DB9::/64

**Answer: A**

### Question 80

Refer to the exhibit.



```
R1#show ip route
1.0.0.0/32 is subnetted, 1 subnets
C 1.1.1.1/32 is directly connected, Loopback0
2.0.0.0/32 is subnetted, 1 subnets
O 2.2.2.2/32 [110/2] via 10.10.10.2, 00:09:30, GigabitEthernet0/0/0
10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C 10.10.10.0/30 is directly connected, GigabitEthernet0/0/0
L 10.10.10.1/32 is directly connected, GigabitEthernet0/0/0
C 10.10.20.0/30 is directly connected, GigabitEthernet0/0/1
```

```
L 10.10.20.1/32 is directly connected, GigabitEthernet0/0/1
D 10.20.10.0/30 [90/3072] via 10.10.10.2, 00:09:30, GigabitEthernet0/0/0
O 10.30.10.0/30 [90/3328] via 10.10.10.2, 00:05:48, GigabitEthernet0/0/0
S 10.40.10.0/30 [1/0] via 10.10.20.2
```

Routers R1, R2, R3, and R4 use EIGRP. However, traffic always prefers R1 to R5 backup links in nonfailure scenarios. Which configuration resolves the issue?

A. R1(config)#no ip route 10.40.10.0 255.255.255.252 10.10.20.2  
R1(config)#ip route 10.40.10.0 255.255.255.252 10.10.20.2 115

B. R1(config)#int gigabitEthernet 0/0/0  
R1 (config-if)#bandwidth 10000000

C. R1(config-if)#int gigabitEthernet 0/0/0  
R1(config-if)#bandwidth 10000

D. R1(config)#no ip route 10.40.10.0 255.255.255.252 10.10.20.2  
R1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2

**Answer: A**

### Question 81

A newly installed spoke router is configured for DMVPN with the **ip mtu 1400** command. Which configuration allows the spoke to use fragmentation with the maximum negotiated TCP MTU over GRE?

- A. ip tcp adjust-mss 1360  
crypto ipsec fragmentation after-encryption
- B. ip tcp adjust-mss 1360  
crypto ipsec fragmentation mtu-discovery
- C. ip tcp payload-mtu 1360  
crypto ipsec fragmentation mtu-discovery
- D. ip tcp payload-mtu 1360  
crypto ipsec fragmentation after-encryption

**Answer: A**

### Question 82

Refer to the exhibit.



```
R1(config)#username Admin password 7 Cisco@123
Invalid encrypted password: Cisco@123
```

An engineer is trying to add an encrypted user password that should not be visible in the router configuration. Which two configuration commands resolve the issue? (Choose two)

- A. service password-encryption
- B. username Admin password 5 Cisco@123
- C. no service password-encryption
- D. username Admin password Cisco@123
- E. password encryption aes
- F. username Admin secret Cisco@123

**Answer: A F**

### Question 83

Refer to the exhibit.

```
access-list 1 permit 209.165.200.215
access-list 2 permit 209.165.200.216
!
interface ethernet 1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip precedence priority
set ip next-hop 209.165.200.217
!
route-map Texas permit 20
match ip address 2
set ip next-hop 209.165.200.218
```

Packets arriving from source 209.165.200.215 must be sent with the precedence bit set to 1, and packets arriving from source 209.165.200.216 must be sent with the precedence bit set to 5. Which action resolves the issue?

- A. set ip precedence immediate in route-map Texas permit 10
- B. set ip precedence priority in route-map Texas permit 20
- C. set ip precedence critical in route-map Texas permit 10
- D. set ip precedence critical in route-map Texas permit 20

**Answer: D**

### **Question 84**

Refer to the exhibit.

```
CPE# ping 10.0.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
CPE# copy flash:/packages.conf tftp://10.0.2.4/
Address or name of remote host [10.0.2.4]?
Destination filename [packages.conf]?
%Error opening tftp://10.0.2.4/packages.conf (Undefined error)
```

The administrator is trying to overwrite an existing file on the TFTP server that was previously uploaded by another router. However, the attempt to update the file fails. Which action resolves this issue?

- A. Make the package.conf file executable by all on the TFTP server.
- B. Make the package.conf file writable by all on the TFTP server.
- C. Make the TFTP folder writable by all on the TFTP server.
- D. Make sure to run the TFTP service on the TFTP server.

**Answer: B**

### **Question 85**

Refer to the exhibit.

R1#sh 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, LI - 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, I - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

D 10.0.0.0/8 [90/409600] via 172.16.1.200, 00:00:28, Ethernet0/0  
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.1.0/24 is directly connected, Ethernet0/0

L 172.16.1.100/32 is directly connected, Ethernet0/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Loopback0

L 192.168.1.100/32 is directly connected, Loopback0

R1#

The R2 loopback interface is advertised with RIP and EIGRP using default values. Which configuration changes make R1 reach the R2 loopback using RIP?

A. R1(config)#router rip

R1 (config-router)#distance 100

B. R1(config)#router rip

R1 (config-router)#distance 90

C. R1(config)#router eigrp 1

R1(config-router)#distance eigrp 120 120

D. R1(config)#router eigrp 1

R1(config-router)#distance eigrp 130 120

**Answer: D**

### **Question 86**

Refer to the exhibit.



R2#show running-config | section ospf

```
ip ospf 1 area 1
ip ospf 1 area 1
router ospf 1
log-adjacency-changes
area 1 stub no summary
R2#show ip ospf interface brief
Interface PID Area IP Address/Mask Cost State Nbrs F/C
Lo0 1 1 10.0.0.2/32 1 Loop 0/0
Fa0/0 1 1 10.10.10.1/30 1 DR 0/1
```

R2#show running-config interface fastEthernet 0/0  
Building configuration...

Current configuration: 116 bytes

```
!
interface FastEthernet0/0
ip address 10.10.10.1 255.255.255.252
ip mtu 1400
ip ospf 1 area 1
duplex full
speed auto
end
```

R2#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.0.0.1	1	EXSTART/BDR	00:00:37	10.10.10.2	FastEthernet0/0

R1#show running-config | section ospf

```
ip ospf 1 area 0
ip ospf 1 area 1
router ospf 1
log-adjacency-changes
area 1 stub no summary
R1#show ip ospf interface brief
Interface PID Area IP Address/Mask Cost State Nbrs F/C
Lo0 1 0 10.0.0.1/32 1 Loop 0/0
Fa1/0 1 1 10.10.10.2/30 1 BDR 0/1
```

R2#show running-config interface fastEthernet 1/0  
Building configuration...

Current configuration: 116 bytes

```
!
interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.252
ip ospf 1 area 1
duplex full
speed auto
end
```

R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.10.10.1	1	EXSTART/DR	00:00:39	10.10.10.1	FastEthernet1/0

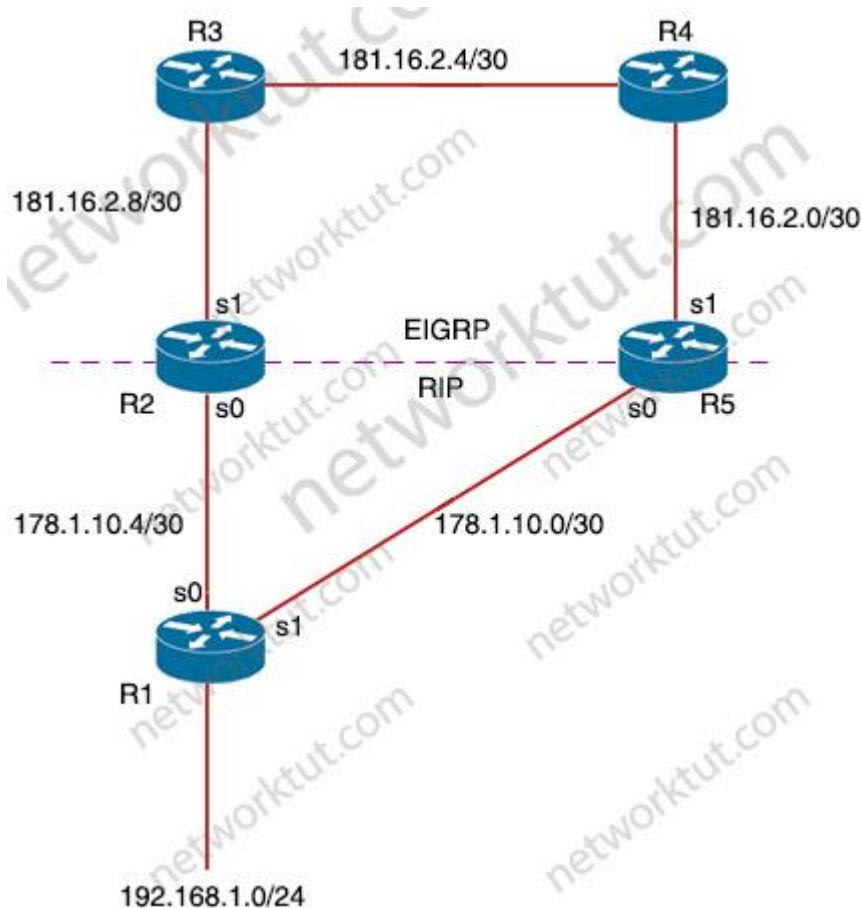
Which action restores OSPF adjacency between R1 and R2?

- A. Change the IP MTU of R1 Fa1/0 to 1300
- B. Change the IP MTU of R2 Fa0/0 to 1300
- C. Change the IP MTU of R1 Fa1/0 to 1500
- D. Change the IP MTU of R2 Fa0/0 to 1500

**Answer: D**

## Question 87

Refer to the exhibit.



Mutual redistribution is enabled between RIP and EIGRP on R2 and R5. Which configuration resolves the routing loop for the 192.168.1.0/24 network?

#### Option A

```
R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
```

#### Option B

```
R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
```

<pre> network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any </pre>	<pre> network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any </pre>
<p><b>Option C</b></p> <p>R2:</p> <pre> router eigrp 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 1 distribute-list 1 in s0 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any </pre> <p>R5:</p> <pre> router eigrp 10 network 181.16.0.0 redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1 ! router rip network 178.1.0.0 redistribute eigrp 10 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any </pre>	<p><b>Option D</b></p> <p>R2:</p> <pre> router eigrp 7 network 181.16.0.0 redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1 ! router rip network 178.1.0.0 redistribute eigrp 7 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any </pre> <p>R5:</p> <pre> router eigrp 7 network 181.16.0.0 redistribute rip metric 1 1 1 1 1 distribute-list 1 in s1 ! router rip network 178.1.0.0 redistribute eigrp 7 metric 2 ! access-list 1 deny 192.168.1.0 access-list 1 permit any </pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

### Question 88

Which IPv6 feature enables a device to reject traffic when it is originated from an address that is not stored in the device binding table?

- A. IPv6 Snooping
- B. IPv6 Source Guard

- C. IPv6 DAD Proxy
- D. IPv6 RA Guard

**Answer: B**

### Question 89

Which IPv6 first hop security feature controls the traffic necessary for proper discovery of neighbor device operation and performance?

- A. RA Throttling
- B. Source or Destination Guard
- C. ND Multicast Suppression
- D. IPv6 Snooping

**Answer: C**

### Question 90

Refer to the exhibit.

```
R1#sh run | s bgp
router bgp 65001
  no synchronization
  bgp router-id 10.100.1.50
  bgp log-neighbor-changes
  network 10.1.1.0 mask 255.255.255.252
  network 10.1.1.12 mask 255.255.255.252
  network 10.100.1.50 mask 255.255.255.255
  timers bgp 20 60
  neighbor R2 peer-group
  neighbor R4 peer-group
  neighbor 10.1.1.2 remote-as 65001
  neighbor 10.1.1.2 peer-group R2
  neighbor 10.1.1.14 remote-as 65001
  neighbor 10.1.1.14 peer-group R4
  no auto-summary
```

While troubleshooting a BGP route reflector configuration, an engineer notices that reflected routes are missing from neighboring routers. Which two BGP configurations are needed to resolve the issue? (Choose two)

- A. neighbor 10.1.1.14 route-reflector-client
- B. neighbor R2 route-reflector-client
- C. neighbor 10.1.1.2 allowas-in
- D. neighbor R4 route-reflector-client
- E. neighbor 10.1.1.2 route-reflector-client

**Answer: B D**

### **Question 91**

An engineer configured a router with this configuration

```
ip access-list DENY_TELNET
 10 deny tcp any any eq 23 log-input
```

The router console starts receiving log message “%SEC-6-IPACCESSLOGP: list DENY\_TELNET denied tcp192.168.1.10(10222) (FastEthernet1/0 D508.89gb.003f) - >192.168.2.20(23), 1 packet”. Which action stops messages on the console while still denying Telnet?

- A. Configure a 20 **permit ip any any** command
- B. Remove **log-input** keyword from the access list.
- C. Replace **log-input** keyword with the **log** keyword in the access list
- D. Configure a 20 **permit ip any any log-input** command.

**Answer: B**

### **Question 92**

What are the two goals of micro BFD sessions? (Choose two)

- A. The high bandwidth member link of a link aggregation group must run BFD.
- B. Run the BFD session with 3×3 ms hello timer.
- C. Continuity for each member link of a link aggregation group must be verified.
- D. Eny member link on a link aggravation group must run BFD.
- E. Each member link of a link aggregation group must run BFD.

**Answer: C E**

### **Question 93**

Refer to the exhibit.

```

ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
 match ip address 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

```

The static route is not present in the routing table of an adjacent OSPF neighbor router. Which action resolves the issue?

- 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**

## New ENARSI Questions 3

### Question 1

Refer to the exhibit.

```

ip prefix-list DefaultRouteOnly seq 5 deny 0.0.0.0/0 le 32
ip prefix-list DefaultRouteOnly seq 10 permit 0.0.0.0/0

router eigrp ccnp
 address-family ipv4 unicast autonomous-system 1
  topology base
  distribute-list prefix DefaultRouteOnly out Tunnel0

```

The administrator configured route advertisement to a remote low resources router to use only the default route to reach any network but failed. Which action resolves this issue?

- A. Change the direction of the distribute-list command from out to in.
- B. Remove the line with the sequence number 10 from the prefix list.
- C. Remove the prefix keyword from the distribute-list command.
- D. Remove the line with the sequence number 5 from the prefix list.

**Answer: D**

### Question 2

Refer to the exhibits. An engineer filtered messages based on severity to minimize log messages.

**Filtered**

```
00:00:35: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:36: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:36: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
```

**Desired**

```
00:00:35: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:36: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:36: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
2 *Jun 1 18:46:11: %SYS-6-CONFIG_I: Configured from console by vty2
```

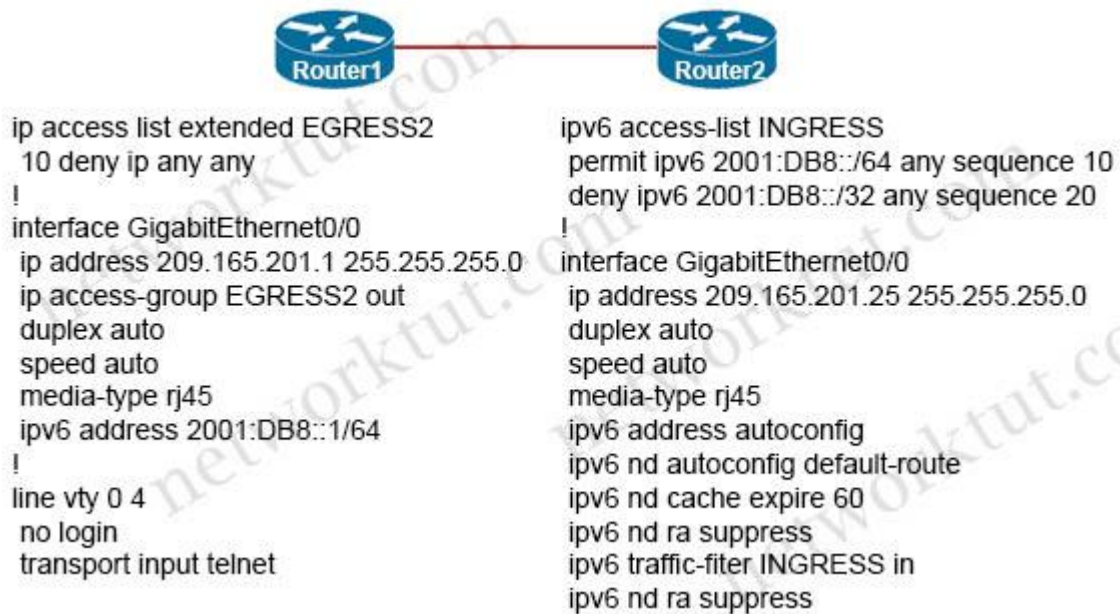
After applying the filter, the engineer noticed that it filtered required messages as well. Which action must the engineer take to resolve the issue?

- A. Configure syslog level 2
- B. Configure syslog level 3
- C. Configure syslog level 4
- D. Configure syslog level 5

**Answer: D**

**Question 3**

Refer to the exhibit. The engineer configured and connected Router2 to Router1. The link came up but could not establish a Telnet connection to Router1 IPv6 address of 2001:DB8::1. Which configuration allows Router2 to establish a Telnet connection to Router1?



- A. IPv6 address on GigabitEthernet0/0
- B. permit ICMPv6 on access list INGRESS for Router2 to obtain IPv6 address
- C. ipv6 unicast-routing
- D. permit ip any any on access list EGRESS2 on Router1

**Answer: A**

#### Question 4

A DMVPN single hub topology is using IPsec + mGRE with OSPF. What should be configured on the hub to ensure it will be the designated router?

- A. route map to set the metrics of learned routes to 110
- B. OSPF priority to 0
- C. OSPF priority greater than 1
- D. tunnel interface of the hub with ip nhrp ospf dr

**Answer: C**

#### Question 5

When configuring Control Plane Policing on a router to protect it from malicious traffic, an engineer observes that the configured routing protocols start flapping on that device. Which action in the Control Plane Policy prevents this problem in a production environment while achieving the security objective?

- A. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the output direction
- B. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit



rates and apply the Control Plane Policy in the input direction

C. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy in the input direction

D. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy in the output direction

**Answer: B**

### Question 6

Refer to the exhibit.

**R1**

```
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
router eigrp 100
 no auto-summary
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.2
```

**R2**

```
interface Loopback0
 ip address 172.16.2.2 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
router eigrp 100
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.1
 passive-interface FastEthernet0/0
```

R1 and R2 cannot establish an EIGRP adjacency. Which action establishes EIGRP adjacency?

A. Add the no auto-summary command to the R2 configuration so that it matches the R1 configuration

B. Remove the passive-interface command from the R2 configuration so that it matches the R1 configuration

C. Add the passive-interface command to the R1 configuration so that it matches the R2 configuration

D. Remove the current autonomous system number on one of the routers and change to a different value

**Answer: B**

### **Question 7**

In which two ways does the IPv6 First-Hop Security Binding Table operate? (Choose two)

- A. by IPv6 routing protocols to securely build neighborships without the need of authentication
- B. by the recovery mechanism to recover the binding table in the event of a device reboot
- C. by IPv6 HSRP to make sure neighbors are authenticated before being used as gateways
- D. by various IPv6 guard features to validate the data link layer address
- E. by storing hashed keys for IPsec tunnels for the built-in IPsec features

**Answer: B D**

### **Question 8**

An engineer configured policy-based routing for a destination IP address that does not exist in the routing table. How is the packet treated through the policy for configuring the **set ip default next-hop** command?

- A. Packets are forwarded to the specific next hop.
- B. Packets are forwarded based on the routing table.
- C. Packets are not forwarded to the specific next hop.
- D. Packets are forwarded based on a static route.

**Answer: A**

### **Question 9**

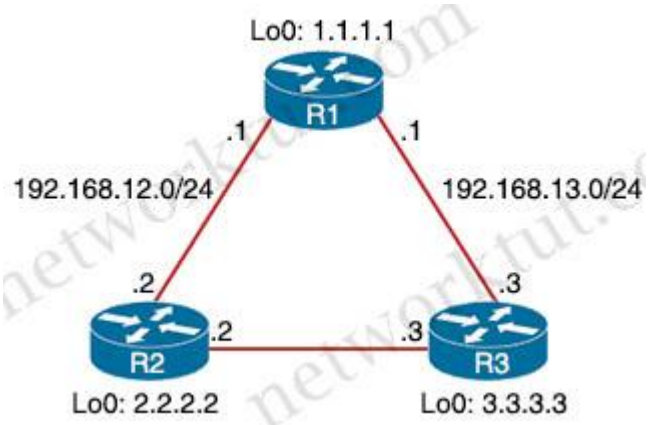
What are two MPLS label characteristics? (Choose two)

- A. A maximum of two labels can be imposed on an MPLS packet.
- B. The label edge router swaps labels on the received packets.
- C. LDP uses TCP for reliable delivery of information.
- D. An MPLS label is a short identifier that identifies a forwarding equivalence class.
- E. Labels are imposed in packets after the Layer 3 header.

**Answer: C D**

### **Question 10**

Refer to the exhibit. R2 has two paths to reach 192.168.13.0/24, but traffic is sent only through R3. Which action allows traffic to use both paths?



```
R2#show ip protocols | include eigrp | Maximum
Routing Protocol is "eigrp 1"
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
```

```
R2#show ip eigrp topology 192.168.13.0/24
EIGRP-IPv4 Topology Entry for AS(1)/ID(2.2.2.2) for 192.168.13.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1075200
Descriptor Blocks:
192.168.23.3 (FastEthernet0/1), from 192.168.23.3, Send flag is 0x0
Composite metric is (1075200/281600), route is Internal
Vector metric:
Minimum bandwidth is 2500 Kbit
Total delay is 2000 microseconds
Reliability is 255/255
Load is 255/255
Minimum MTU is 1500
Hop count is 1
Originating router is 3.3.3.3
192.168.12.1 (FastEthernet0/0), from 192.168.12.1, Send flag is 0x0
Composite metric is (2611200/281600), route is Internal
Vector metric
Minimum bandwidth is 1000 Kbit
Total delay is 2000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 1
Originating router is 1.1.1.1
```

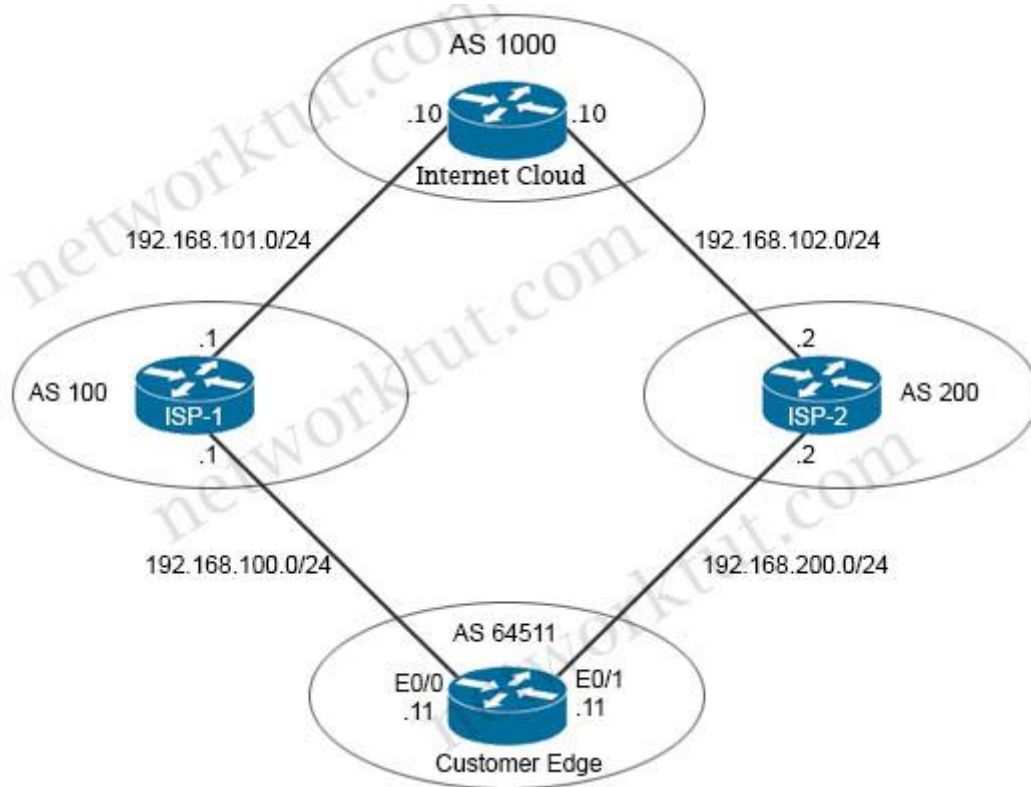
```
R2#show ip route 192.168.13.0
Routing entry for 192.168.13.0/24
Known via "eigrp 1", distance 90, metric 1075200, type internal
Redistributing via eigrp 1
Last update from 192.168.23.3 on FastEthernet0/1, 00:00:57 ago
Routing Descriptor Blocks:
* 192.168.23.3, from 192.168.23.3, 00:00:57 ago, via FastEthernet0/1
Route metric a 1075200, traffic share count is 1
Total delay is 2000 microseconds, minimum bandwidth is 2500 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 255/255, Hops 1
```

- A. Configure the **bandwidth 2000** command under interface FastEthernet0/0 on R2
- B. Configure the **delay 1** command under interface FastEthernet0/0 on R2
- C. Configure the **variance 2** command under the EIGRP process on R2
- D. Configure the **variance 4** command under the EIGRP process on R2

**Answer: D**

**Question 11**

Refer to the exhibit.



The network administrator has configured the Customer Edge router (AS 64511) to send only summarized routes toward ISP-1 (AS 100) and ISP-2 (AS 200).

```
router bgp 64511
 network 172.16.20.0 mask 255.255.255.0
 network 172.16.21.0 mask 255.255.255.0
 network 172.16.22.0 mask 255.255.255.0
 network 172.16.23.0 mask 255.255.255.0
 aggregate-address 172.16.20.0 255.255.252.0
```

After this configuration, ISP-1 and ISP-2 continue to receive the specific routes and the summary route. Which configuration resolves the issue?

A. router bgp 64511  
aggregate-address 172.16.20.0 255.255.252.0 summary-only

B. router bgp 64511  
neighbor 192.168.100.1 summary-only  
neighbor 192.168.200.2 summary-only

C. interface E0/0  
ip bgp suppress-map BLOCK\_SPECIFIC  
!  
interface E0/1  
ip bgp suppress-map BLOCK\_SPECIFIC  
!

```
ip prefix-list PL_BLOCK_SPECIFIC
permit 172.16.20.0/22 ge 24
!
route-map BLOCK_SPECIFIC permit 10
match ip address prefix-list PL_BLOCK_SPECIFIC
```

```
D. ip prefix-list PL_BLOCK_SPECIFIC
deny 172.16.20.0/22 ge 22
ip prefix-list PL_BLOCK_SPECIFIC
permit 172.16.20.0/22
!
route-map BLOCK_SPECIFIC permit 10
match ip address prefix-list PL_BLOCK_SPECIFIC
!
router bgp 64511
aggregate-address 172.16.20.0 255 255.252.0 suppress-map BLOCK_SPECIFIC
```

**Answer: A**

## Question 12

Refer to the exhibit.

### Configuration output:

```
clock timezone PST -8
clock summer-time PDT recurring
service timestamps debug datetime
service timestamps log datetime
logging buffered 16000 debugging
ntp clock-period 17178272
ntp server 161.181.92.152
```

### Debug output:

```
router#show clock
14:12:26:312 PDT Thu Apr 27 2019
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#exit

router#
Apr 27 21:12:28: %SYS-5-CONFIG_I: Configured from console by vty0
```

A network administrator configured NTP on a Cisco router to get synchronized time for system and logs from a unified time source. The configuration did not work as desired. Which service must be enabled to resolve the issue?

- A. Enter the **service timestamps log datetime clock-period** global command
- B. Enter the **service timestamps log datetime synchronize** global command
- C. Enter the **service timestamps log datetime console** global command
- D. Enter the **service timestamps log datetime localtime** global command

**Answer: D**

### Question 13

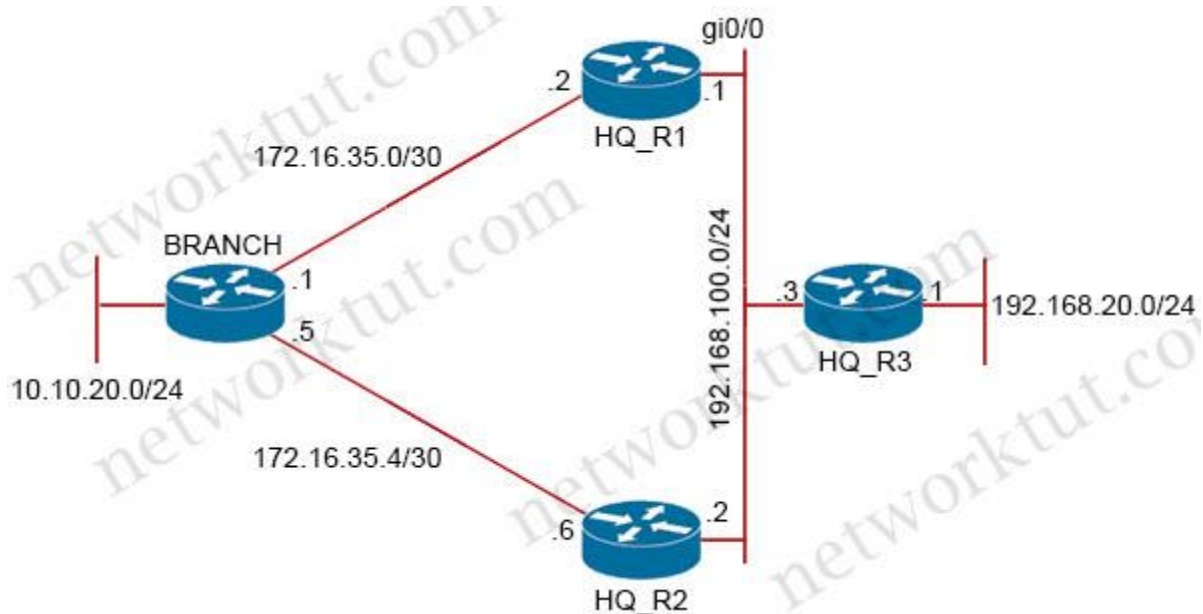
What are two functions of MPLS Layer 3 VPNs? (Choose two)

- A. BGP is used for signaling customer VPNv4 routes between PE nodes.
- B. It is used for transparent point-to-multipoint connectivity between Ethernet links/sites.
- C. LDP and BGP can be used for Pseudowire signaling.
- D. A packet with node segment ID is forwarded along with shortest path to destination.
- E. Customer traffic is encapsulated in a VPN label when it is forwarded in MPLS network.

**Answer: A E**

### Question 14

Refer to the exhibit.



```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
!
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.2
BRANCH(config-ip-sla)# timeout 200
```

```
BRANCH(config-ip-sla)# frequency 5
!  
BRANCH(config)#ip sla schedule 1 life forever start-time now
!  
BRANCH(config)# track 1 ip sla 1 reachability
```

An engineer has successfully set up a floating static route from the BRANCH router to the HQ network using HQ\_R1 as the primary default gateway. When the g0/0 goes down on HQ\_R1, the branch network cannot reach the HQ network 192.168.20.0/24. Which set of configurations resolves the issue?

- A. BRANCH(config)# ip sla 1  
BRANCH(config-ip-sla)# icmp-echo 192.168.100.2
- B. BRANCH(config)# ip sla 1  
BRANCH(config-ip-sla)# icmp-echo 192.168.100.1
- C. HQ\_R3(config)# ip sla responder  
HQ\_R3(config)# ip sla responder icmp-echo 172.16.35.5
- D. HQ\_R3(config)# ip sla responder  
HQ\_R3(config)# ip sla responder icmp-echo 172.16.35.1

**Answer: B**

### Question 15

Refer to the exhibit. Which action restores the routes from neighbors while still filtering 1.1.1.0/24?

```
access-list 1 permit 1.1.1.0 0.0.0.255
!  
route-map FILTER1 deny 10  
  match ip address 1  
!  
router eigrp 1  
  distribute-list route-map FILTER1 in
```

- A. Modify the access list to deny instead of permit it
- B. Modify the route map to permit the access list instead of deny it
- C. Add a second sequence in the route map permit 20
- D. Add a second line in the access list to permit any

**Answer: C**

### Question 16



An engineer configured two routers connected to two different service providers using BGP with default attributes. One of the links is presenting high delay, which causes slowness in the network. Which BGP attribute must the engineer configure to avoid using the high-delay ISP link if the second ISP link is up?

- A. WEIGHT
- B. MED
- C. LOCAL\_PREF
- D. AS-PATH

**Answer: C**

### **Question 17**

An engineer configured a DHCP server for Cisco IP phones to download its configuration from a TFTP server, but the IP phones failed to load the configuration. What must be configured to resolve the issue?

- A. DHCP option 66
- B. BOOTP port 67
- C. BOOTP port 68
- D. DHCP option 69

**Answer: A**

### **Question 18**

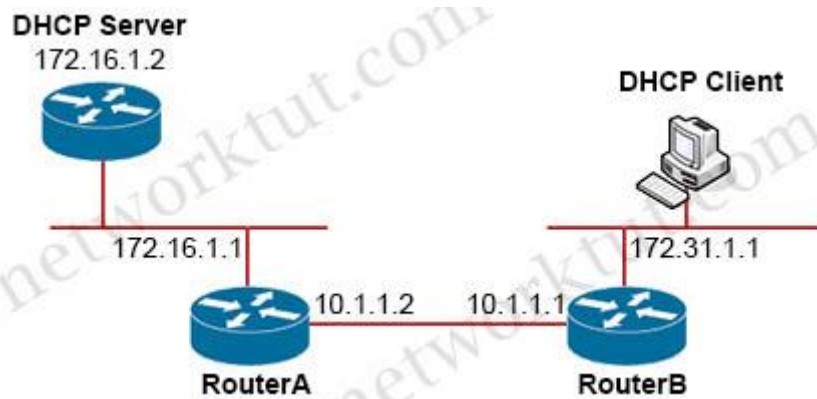
What are two purposes of using IPv4 and VPNv4 address-family configurations in a Layer 3 MPLS VPN? (Choose two)

- A. The VPNv4 address is used to advertise the MPLS VPN label.
- B. RD is prepended to the IPv4 route to make it unique.
- C. MP-BGP is used to allow overlapping IPv4 addresses between customers to advertise through the network.
- D. The IPv4 address is needed to tag the MPLS label.
- E. The VPNv4 address consists of a 64-bit route distinguisher that is prepended to the IPv4 prefix.

**Answer: B E**

### **Question 19**

Refer to the exhibit.



The DHCP client is unable to receive an IP address from the DHCP server. RouterB is configured as follows:

```
interface FastEthernet0/0
  description Client DHCP ID 43574645
  ip address 172.31.1.1 255.255.255.0
  !
ip route 172.16.1.0 255.255.255.0 10.1.1.2
```

Which command is required on the FastEthernet0/0 interface of RouterB to resolve this issue?

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

**Answer: B**

## Question 20

Refer to the exhibit.

```
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt 0x52 flag 0x7 len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1 [10]
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt 0x52 flag 0x7 len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1 [11]
%OSPF-5-ADJCHG: Process 1, Nbr 10.100.1.2 on GigabitEthernet0/1 from EXSTART to
DOWN, Neighbor Down: Too many retransmissions
```

The OSPF neighbor relationship is not coming up. What must be configured to restore OSPF neighbor adjacency?

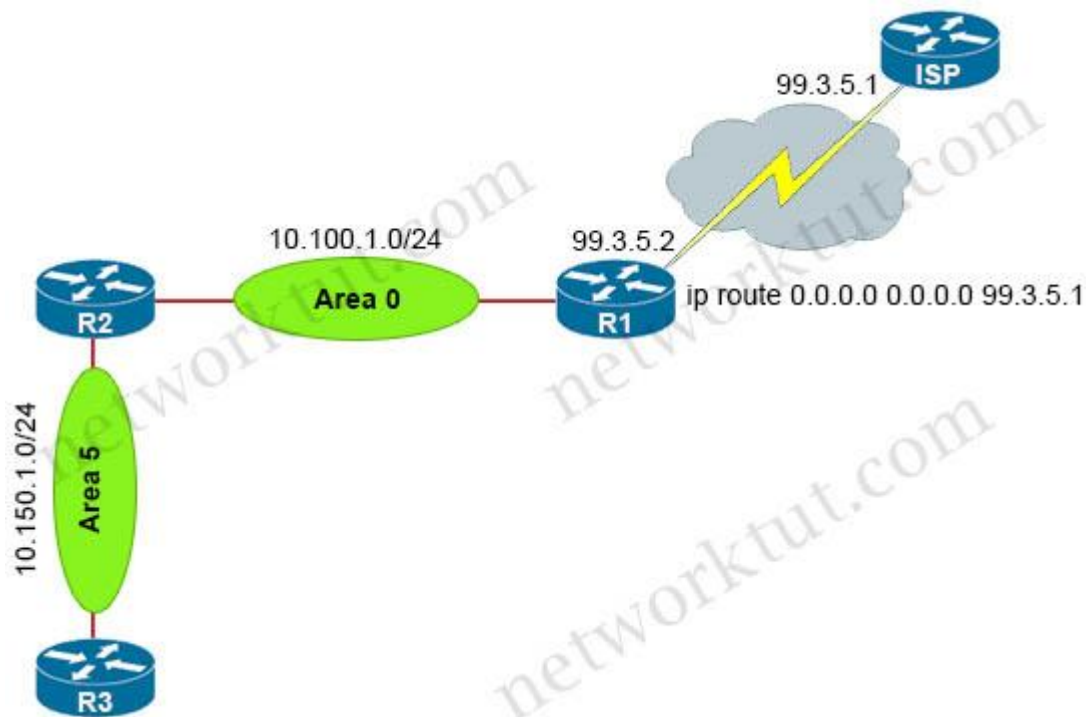
- A. matching hello timers
- B. matching MTU values

- C. use router ID
- D. OSPF on the remote router

**Answer: B**

### Question 21

Refer to the exhibit.



A network administrator redistributed the default static route into OSPF toward all internal routers to reach to Internet. Which set of commands restores reachability to the Internet by internal routers?

- A. router ospf 1  
redistribute static subnets
- B. router ospf 1  
network 0.0.0.0 0.0.0.0 area 0
- C. router ospf 1  
redistribute connected 0.0.0.0
- D. router ospf 1  
default-information originate

**Answer: D**

## **Question 22**

Refer to the exhibit.

```
ipv6 unicast-routing
!
router ospfv3 4
  router-id 192.168.1.1
!
interface E0/0
  ipv6 enable
  ip address 10.1.1.1 255.255.255.0
  ospfv3 4 area 0 ipv4
  no shut
!
interface Loopback0
  ipv6 enable
  ipv4 172.16.1.1 255.255.255.0
  ospfv3 4 area 0 ipv4
```

The network administrator configured the branch router for IPv6 on the E0/0 interface. The neighboring router is fully configured to meet requirements, but the neighbor relationship is not coming up. Which action fixes the problem on the branch router to bring the IPv6 neighbors up?

- A. Enable the IPv4 address family under the **router ospfv3 4** process by using the **address-family ipv4 unicast** command
- B. Disable IPv6 on the E0/0 interface using the **no ipv6 enable** command
- C. Enable the IPv4 address family under the E0/0 interface by using the **address-family ipv4 unicast** command
- D. Disable OSPF for IPv4 using the **no ospfv3 4 area 0 ipv4** command under the E0/0 interface

**Answer: A**

## **Question 23**

What are two characteristics of VRF instance? (Choose two)

- A. All VRFs share customers routing and CEF tables
- B. Each VRF has a different set of routing and CEF tables
- C. An interface must be associated to one VRF
- D. A customer site can be associated to different VRFs
- E. It is defined by the VPN membership of a customer site attached to a P device

**Answer: B D**

## **Question 24**

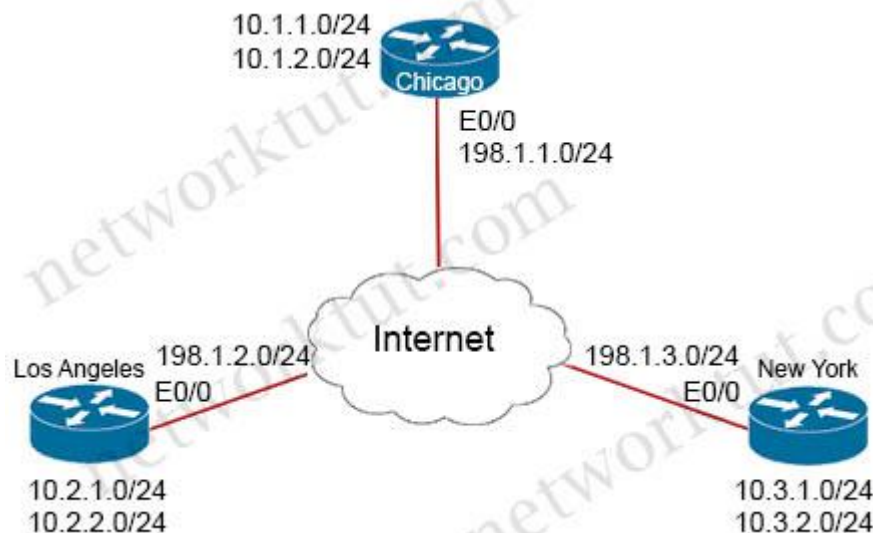
Which two components are needed for a service provider to utilize the L3VPN MPLS application? (Choose two)

- A. The P routers must be configured with RSVP
- B. The P routers must be configured for MP-iBGP toward the PE routers
- C. The P and PE routers must be configured with LDP or RSVP
- D. The PE routers must be configured for MP-eBGP to connect to CEs
- E. The PE routers must be configured for MP-iBGP with other PE routers

**Answer:** C E

### Question 25

Refer to the exhibit. The Los Angeles and New York routers are receiving routes from Chicago but not from each other. Which configuration fixes the issue?



#### Chicago

```
interface Tunnel 1
 ip address 192.168.1.1255.255.255.0
 tunnel source E0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp map multicast dynamic
 no ip next-hop-self eigrp 111
 tunnel protection ipsec profile IPSec-PROFILE
!
router eigrp 111
 network 192.168.1.0
 network 10.0.0.0
```

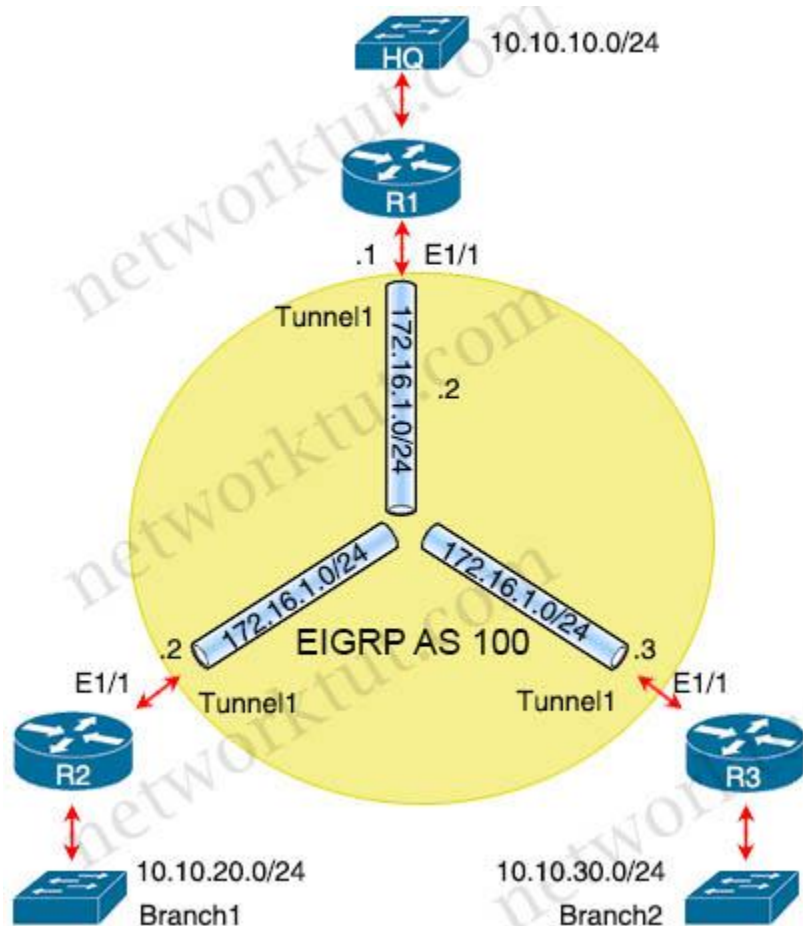
- A. interface Tunnel1
- ip next-hop-self eigrp 111

- ```
D. interface Tunnel1
 tunnel protection ipsec profile IPSec-PROFILE
```

**Answer: B**

### Question 26

Refer to the exhibit.



An engineer sets up a DMVPN connection to connect branch 1 and branch 2 to HQ branch 1 and branch 2 cannot communicate with each other. Which change must be made to resolve this issue?

- ```
A. R1(config)#int e1/1
R1(config-if)#no ip split-horizon eigrp 100
```

B. R1(config)#int tunnel1  
R1(config-if)#no ip split-horizon eigrp 100

C. R1(config)#router eigrp 100  
R1(config-if)#neighbor 172.16.1.3

D. R1(config)#router eigrp 100  
R1(config-if)#neighbor 172.16.1.2

**Answer: B**

### Question 27

What is the minimum time gap required by the local system before putting a BFD control packet on the wire?

- A. Required Min RX Interval
- B. Required Min Echo RX Interval
- C. Detect Mult
- D. Desired Min TX Interval

**Answer: D**

### Question 28

Refer to exhibit.

```
ip dhcp excluded-address 172.16.16.1 172.16.16.2
!
ip dhcp pool 0
 network 172.16.16.0 255.255.255.0
 domain-name networktut.com
 dns-server 172.16.16.2
 lease 30

interface Ethernet0/0
 ip address 10.1.1.1255.255.255.252
 ip access-group 100 in

access-list 100 deny udp any any
access-list 100 permit ip any any
```

Which two configurations allow clients to get dynamic ip addresses assigned? (Choose two)

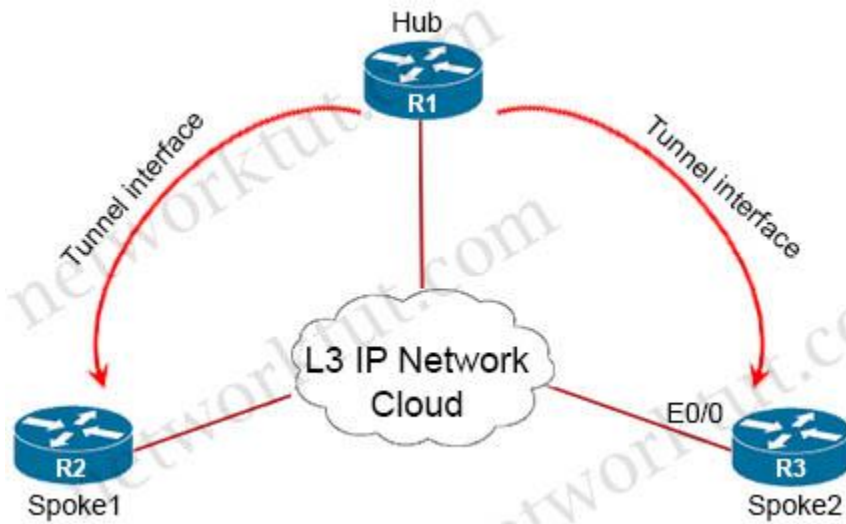
- A. Configure access-list 100 permit udp any any eq 68 as the first line
- B. Configure access-list 100 permit udp any any eq 86 as the first line
- C. Configure access-list 100 permit udp any any eq 61 as the first line

- D. Configure access-list 100 permit udp any any eq 67 as the first line
- E. Configure access-list 100 permit udp any any eq 69 as the first line

**Answer:** A D

### Question 29

Refer to exhibit.



A network administrator has successfully configured DMVPN topology between a hub and two spoke routers. Which two configuration commands should establish direct communications between spoke 1 and spoke 2 without going through the hub? (Choose two)

- A. At the hub router, configure the **ip nhrp shortcut** command
- B. At the hub router, configure **ip nhrp redirect** command
- C. At the hub router, configure the **ip nhrp spoke-tunnel** command
- D. At the spoke routers, configure the **ip nhrp shortcut** command
- E. At the spoke routers, configure the **ip nhrp spoke-tunnel** command

**Answer:** B D

### Question 30

Which IPv6 first-hop security feature helps to minimize denial of service attacks?

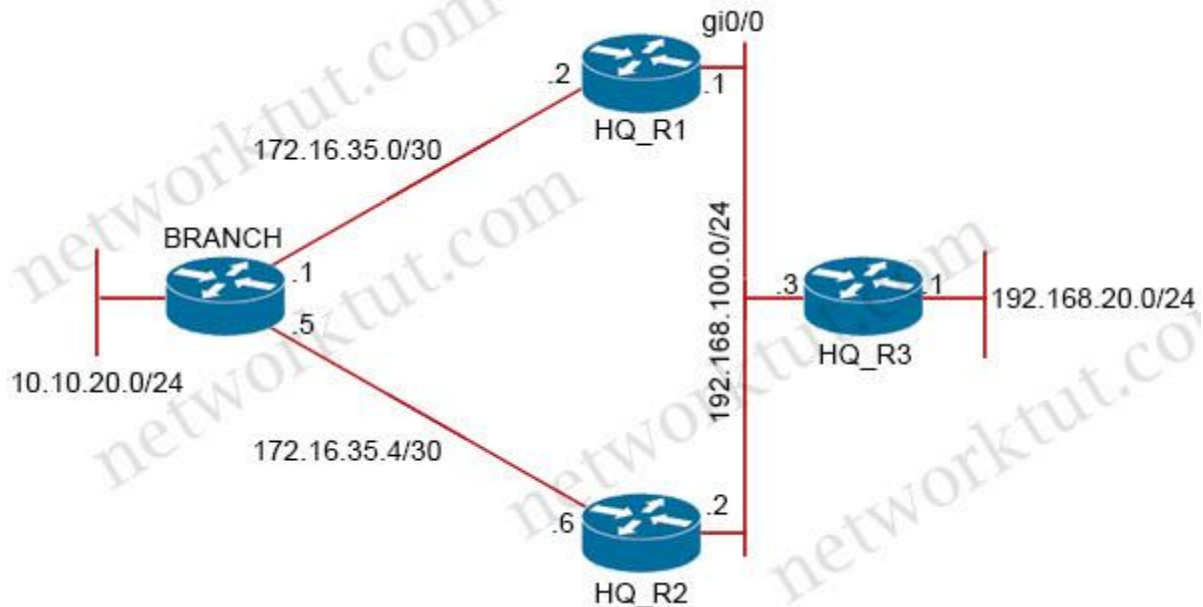
- A. IPv6 Router Advertisement Guard
- B. IPv6 Destination Guard
- C. DHCPv6 Guard
- D. IPv6 MAC address filtering



**Answer: B**

### Question 31

Refer to the exhibit.



```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
!
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.6
BRANCH(config-ip-sla)# timeout 200
BRANCH(config-ip-sla)# frequency 5
!
BRANCH(config)# ip sla schedule 1 life forever start-time now
!
BRANCH(config)# track 1 ip sla 1 reachability
```

Traffic from the branch network should route through HQ\_R1 unless the path is unavailable. An engineer tests this functionality by shutting down interface on the BRANCH router toward HQ\_R1 router but 192.168.20.0/24 is no longer reachable from the branch router.

Which set of configurations resolves the issue?

A. HQ\_R2(config)# ip sla responder  
HQ\_R2(config)# ip sla responder icmp-echo 172.16.35.5

B. BRANCH(config)# ip sla 1  
BRANCH(config-ip-sla)# icmp-echo 172.16.35.1

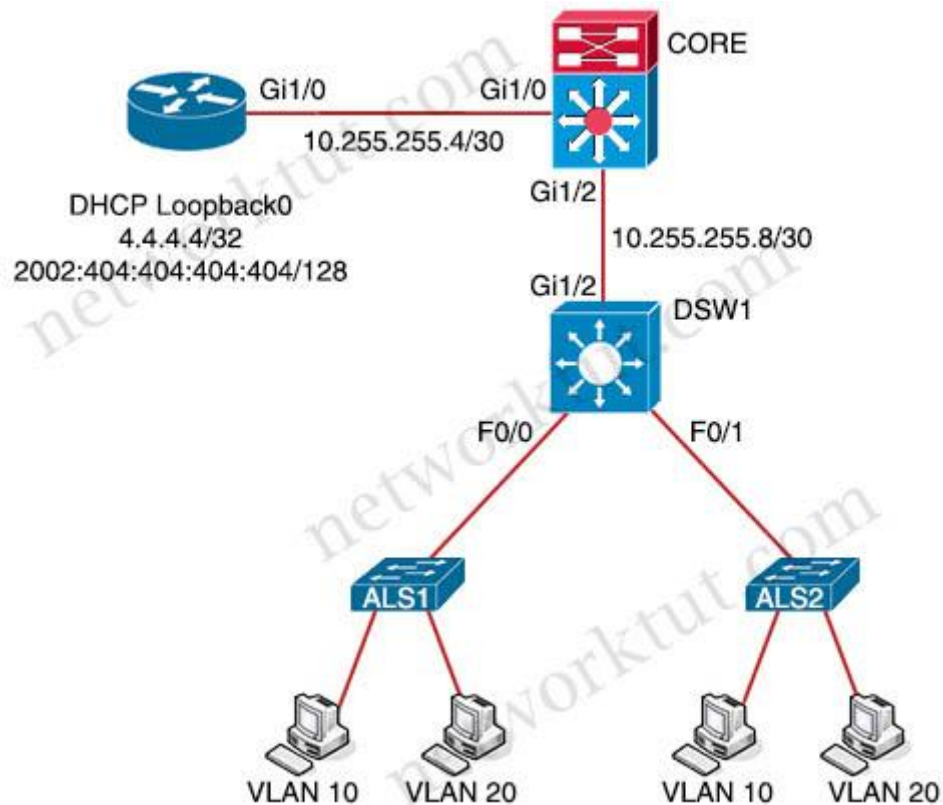
C. HQ\_R1(config)# ip sla responder  
HQ\_R1(config)# ip sla responder icmp-echo 172.16.35.2

D. BRANCH(config)# ip sla 1  
BRANCH(config-ip-sla)# icmp-echo 172.16.35.2

**Answer: D**

### Question 32

Refer to the exhibit.



```
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
```

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?

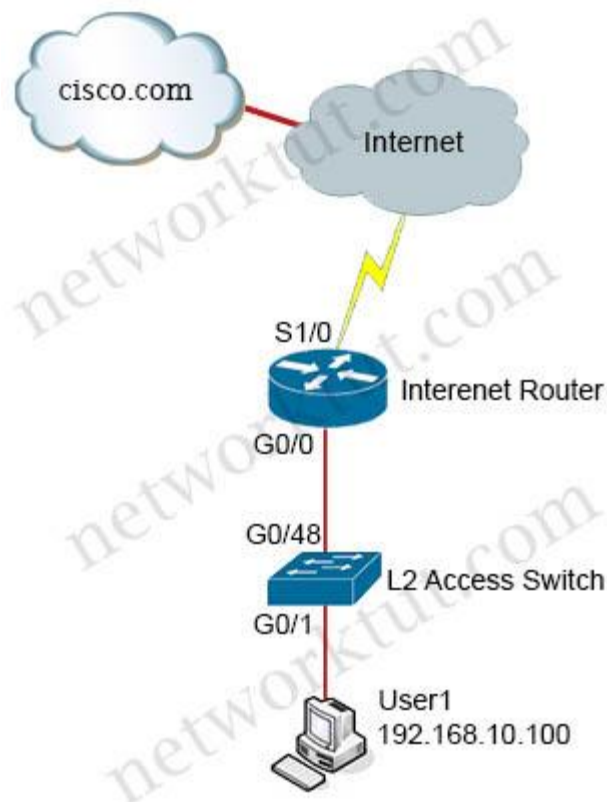
- A. DSW1(dhcp-config)# default-router 2002:A04:A01::A04:A01
- B. DSW1(config)#ipv6 route 2002:404:404::404:404/128 FastEthernet 1/0

- C. DSW1(config)# ipv6 dhcp relay destination 2002:404:404::404:404 GigabitEthernet 1/2  
D. DSW1(config-if)# ipv6 helper address 2002:404:404::404:404

**Answer: C**

### Question 33

A network administrator is tasked to permit http and https traffic only toward the internet from the User1 laptop to adhere to company's security policy. The administrator can still ping to www.cisco.com. Which interface should the access list 101 be applied to resolve this issue?



```
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 80
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 443
access-list 101 deny ip any any log
!
interface Serial1/0
 ip address 200.193.22.94 255.255.255.252
 ip access-group 101 in
```

- A. Interface G0/48 in the incoming direction  
B. Interface G0/0 in the incoming direction  
C. Interface S1/0 in the outgoing direction  
D. Interface G0/0 in the outgoing direction

**Answer: B**

### Question 34

Refer to the exhibit.

```
config t

flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 2055
exit
!
flow monitor FLOW-MONITOR-1
exporter EXPORTER-1
record v4_r1
exit
!
flow monitor v4_r1
!
ip cef
!

interface Ethernet0/0.1
ip address 172.16.6.2 255.255.255.0
ip flow monitor v4_r1 input
```

The remote server is failing to receive the NetFlow data. Which action resolves the issue?

- A. Modify the flow transport command **transport udp 2055** to move under flow monitor profile.
- B. Modify the interface command to **ip flow monitor FLOW-MONITOR-1 input**.
- C. Modify the udp port under flow exporter profile to ip transport udp 4739.
- D. Modify the flow record command record v4\_M to move under flow exporter profile.

**Answer: B**

### Question 35

An engineer must configure a Cisco router to initiate secure connections from the router to other devices in the network but kept failing. Which two actions resolve the issue? (Choose two)

- A. Configure a domain name.
- B. Configure a crypto key to be generated.
- C. Configure a TACACS+ server and enable it.
- D. Configure transport input ssh command on the console.
- E. Configure a source port for the SSH connection to initiate.

**Answer: A B**

### Question 36

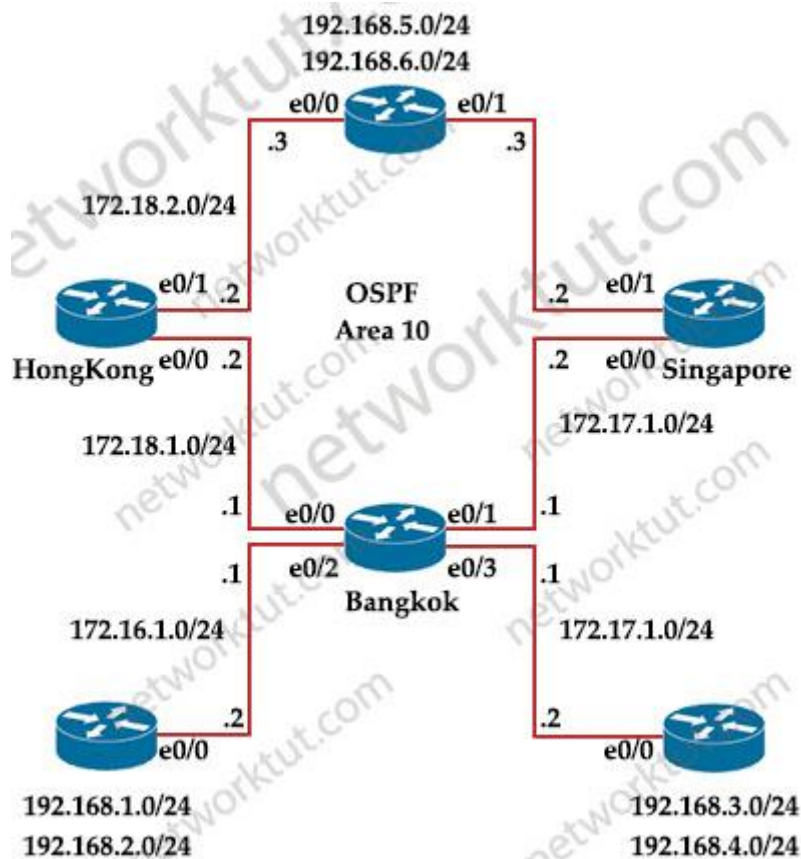
An engineer is troubleshooting on the console session of a router and turns on multiple debug commands. The console screen is filled with scrolling debug messages that none of the commands can be verified if entered correctly or display any output. Which action allows the engineer to see entered console commands while still continuing the analysis of the debug messages?

- A. Configure the no logging console debugging command globally
- B. Configure the logging synchronous command
- C. Configure the logging synchronous level all command
- D. Configure the term no mon command globally

**Answer: B**

### Question 37

Bangkok is using ECMP to reach to the 192.168.5.0/24 network. The administrator must configure Bangkok in such a way that Telnet traffic from 192.168.3.0/24 and 192.168.4.0/24 networks uses the HongKong router as the preferred router. Which set of configurations accomplishes this task?



A . access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255  
 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255  
 !

route-map PBR1 permit 10  
 match ip address 101  
 set ip next-hop 172.18.1.2  
 interface Ethernet0/3  
 ip policy route-map PBR1

B. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23  
 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23  
 !

route-map PBR1 permit 10  
 match ip address 101  
 set ip next-hop 172.18.1.2  
 interface Ethernet0/1  
 ip policy route-map PBR1

C. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23  
 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23  
 !

route-map PBR1 permit 10  
 match ip address 101  
 set ip next-hop 172.18.1.2  
 !

```
interface Ethernet0/3
ip policy route-map PBR1
```

```
D. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
!
interface Ethernet0/1
ip policy route-map PBR1
```

**Answer: C**

### Question 38

Refer to the exhibit.

```
11:27:07.532: AAA/BIND (00000055): Bind i/
11:27:07.532: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
11:27:07.532: TPLUS: Queuing AAA Authentication request 85 for processing
11:27:07.532: TPLUS (00000055) login timer started 1020 sec timeout
11:27:07.532: TPLUS: processing authentication start request id 85
11:27:07.532: TPLUS: Authentication start packet created for 85()
11:27:07.532: TPLUS: Using server 10.106.60.182
11:27:07.532: TPLUS (00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: socket event 2
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: wrote entire 38 bytes request
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: Would block while reading
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
13:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: read entire 18 bytes response
11:27:07.532: TPLUS (00000055)/0/225FE2DC: Processing the reply packet
11:27:07.532: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
11:27:07.532: TPLUS: Invalid AUTHEN packet (check keys).
```

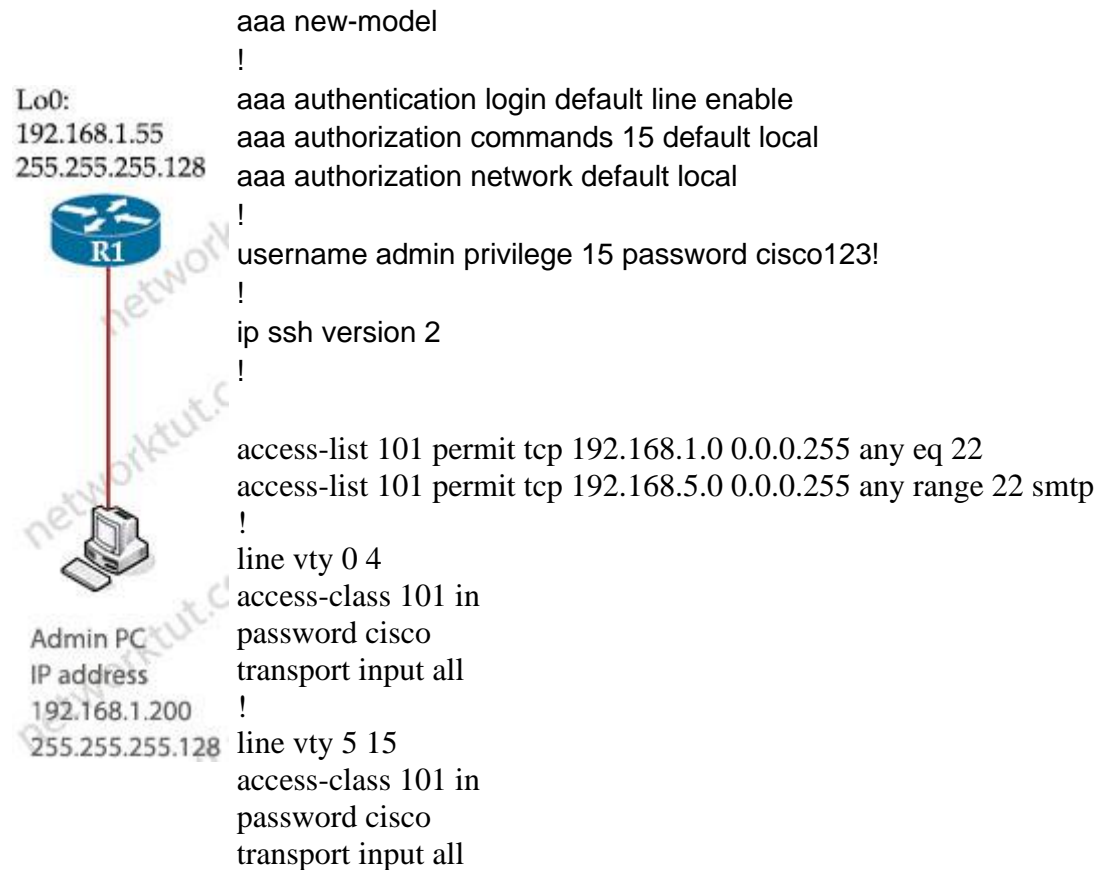
Which action resolves the authentication problem?

- A. Configure the user name on the TACACS+ server
- B. Configure the UDP port 1812 to be allowed on the TACACS+ server
- C. Configure the TCP port 49 to be reachable by the router
- D. Configure the same password between the TACACS+ server and router.

**Answer: D**

### Question 39

Refer to the exhibit.



The administrator successfully logs into R1 but cannot access privileged mode commands. What should be configured to resolve the issue?

- A. aaa authorization reverse-access
- B. secret cisco123! at the end of the username command instead of password cisco123!
- C. matching password on vty lines as cisco123!
- D. enable secret or enable password commands to enter into privileged mode

**Answer: D**

### Question 40

Drag and drop the MPLS concepts from the left onto the descriptions on the right.



label edge router	allows an LSR to remove the label before forwarding the packet
label switch router	accepts unlabeled packets and imposes labels
forwarding equivalence class	group of packets that are forwarded in the same manner
penultimate hop popping	receives labeled packets and swaps labels

**Answer:**

- + allows an LSR to remove the label before forwarding the packet: penultimate hop popping
- + accepts unlabeled packets and imposes labels: label edge router
- + group of packets that are forwarded in the same manner: forwarding equivalence class
- + receives labeled packets and swaps labels: label switch router

**Question 41**

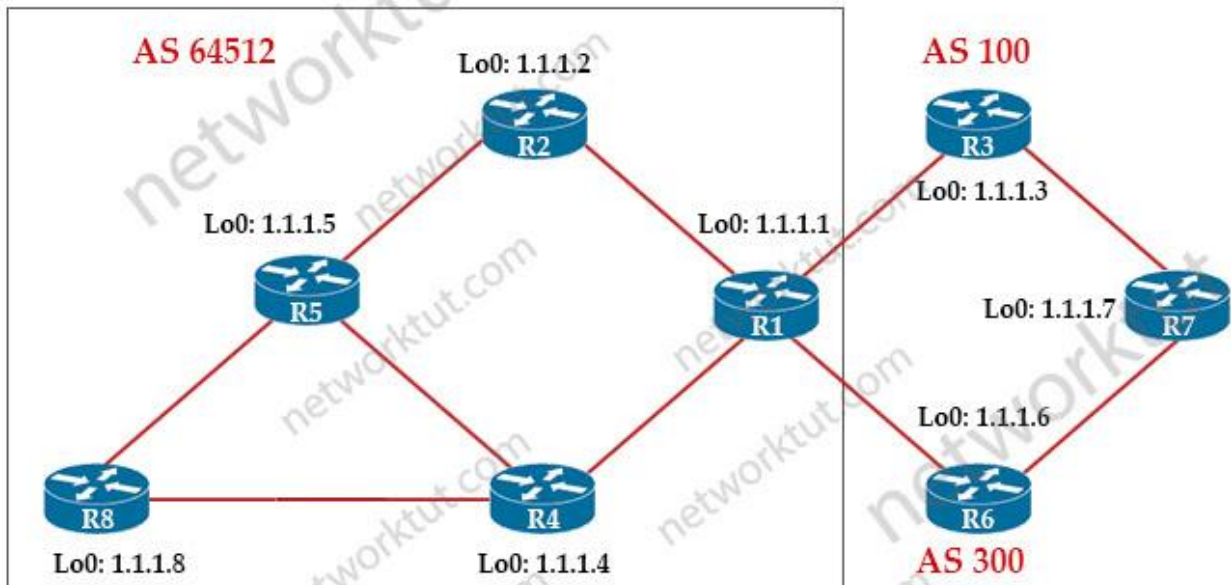
Which two protocols work in the control plane of P routers across the MPLS cloud? (choose two)

- A. LSP
- B. RSVP
- C. ECMP
- D. LDP
- E. MPLS OAM

**Answer:** B D

**Question 42**

Refer to the exhibit.



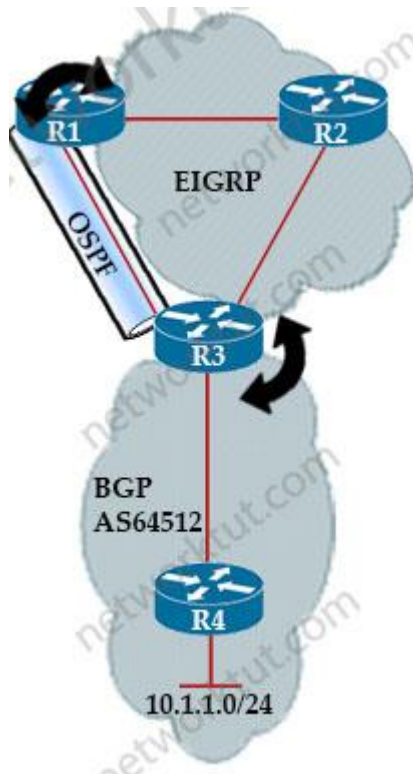
An engineer configured R2 and R5 as route reflectors and noticed that not all routes are sent to R1 to advertise to the eBGP peers. Which iBGP routers must be configured as route reflectors to advertise all routes to restore reachability across all networks?

- A. R1 and R4
- B. R1 and R5
- C. R4 and R5
- D. R2 and R5

**Answer:** C

#### Question 43

Refer to the exhibit.



Routing protocols are mutually redistributed on R3 and R1. Users report intermittent connectivity to services hosted on the 10.1.1.0/24 prefix. Significant routing update changes are noticed on R3 when the **show ip route profile** command is run. How must the services be stabilized?

- A. The issue with using BGP must be resolved by using another protocol and redistributing it into EIGRP on R3
- B. The routing loop must be fixed by reducing the admin distance of iBGP from 200 to 100 on R3
- C. The routing loop must be fixed by reducing the admin distance of OSPF from 110 to 80 on R3
- D. The issue with using iBGP must be fixed by running eBGP between R3 and R4

**Answer: B**

#### **Question 44**

Refer to the exhibit.



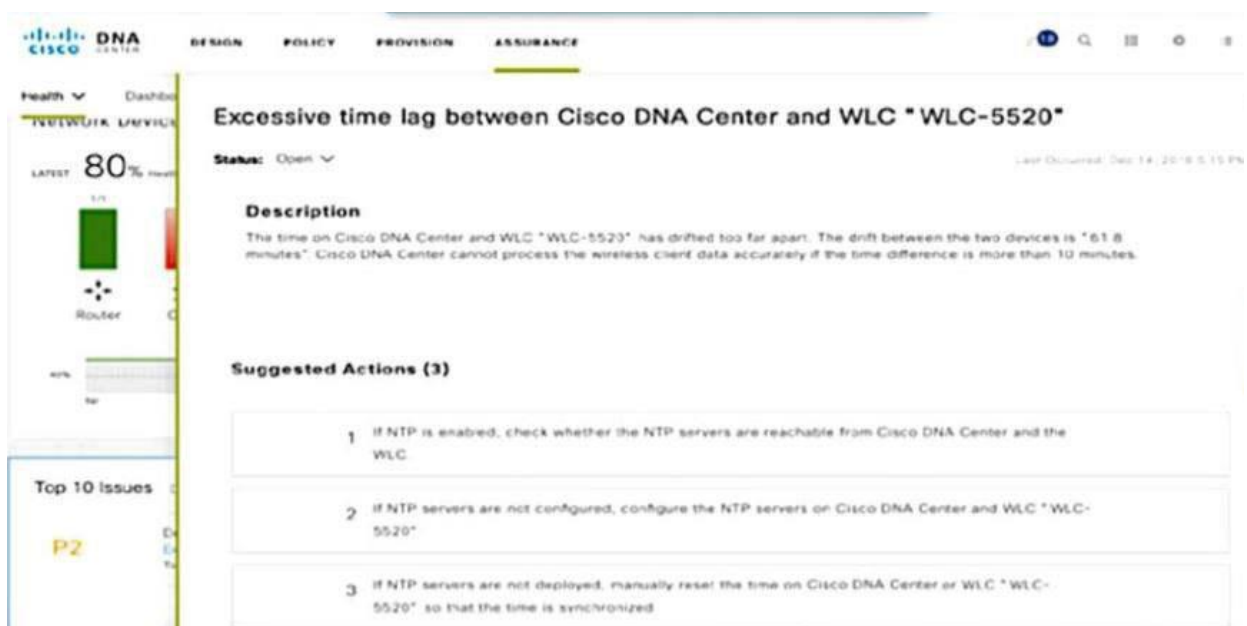
A network administrator added one router in the Cisco DNA Center and checked its discovery and health from the Network Health Dashboard. The network administrator observed that the router is still showing up as unmonitored. What must be configured on the router to mount it in the Cisco DNA Center?

- A. Configure router with NetFlow data
- B. Configure router with the telemetry data
- C. Configure router with routing to reach Cisco DNA Center
- D. Configure router with SNMPv2c or SNMPv3 traps

**Answer: B**

## Question 45

Refer to the exhibit.



NTP is configured across the network infrastructure and Cisco DNA Center. An NTP issue was reported on the Cisco DNA Center at 17:15. Which action resolves the issue?

- A. Check and resolve reachability between the WLC and the NTP server
- B. Reset the NTP server to resolve any synchronization issues for all devices
- C. Check and resolve reachability between Cisco DNA Center and the NTP server
- D. Check and configure NTP on the WLC and synchronize with Cisco DNA Center

**Answer: D**

### Question 46

Refer to the exhibit.

```
Feb 9:15:29:29.713: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPINFORM, input interface:
Po2, MAC da: ffff.ffff.ffff, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP
giaddr: 0.0.0.0
Feb 9:15:29:29.713: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is
flooded to ingress VLAN (1)
Feb 9:15:29:29.713: DHCP_SNOOPING_SW: bridge packet send packet to cpu port:
Vlan1.
Feb 9:15:29:31.223: DHCP Snooping(hlrm_set_if_input): Setting if_input to Po2 for
pak. Was V11
Feb 9:15:29:31.223: DHCP Snooping(hlrm_set_if_input): Setting if_input to V11 for
pak. Was Po2
Feb 9:15:29:31.223: DHCP Snooping(hlrm_set_if_input): Setting if_input to Po2 for
pak. Was V11
Feb 9:15:29:31.223: DHCP_SNOOPING: received new DHCP packet from input
interface (Port-channel2)
```

A network administrator enables DHCP snooping on the Cisco Catalyst 3750-X switch and configures the uplink port (Port-channel2) as a trusted port. Clients are not receiving an IP address, but when DHCP snooping is disabled, clients start receiving IP addresses. Which global command resolves the issue?

- A. No ip dhcp snooping information option
- B. ip dhcp snooping
- C. ip dhcp relay information trust portchannel2
- D. ip dhcp snooping trust

**Answer: A**

### Question 47

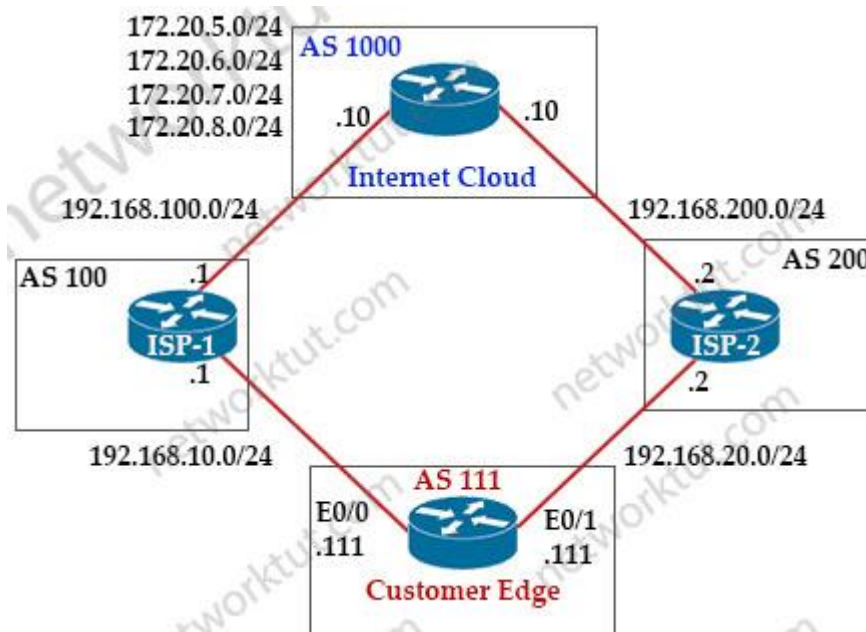
Which configuration feature should be used to block rogue router advertisements instead of using the IPv6 Router Advertisement Guard feature?

- A. VACL blocking broadcast frames from nonauthorized hosts
- B. PVLANS with promiscuous ports associated to route advertisements and isolated ports for nodes
- C. PVLANS with community ports associated to route advertisements and isolated ports for nodes
- D. IPv4 ACL blocking route advertisements from nonauthorized hosts

**Answer: B**

### Question 48

Refer to the exhibit.



```
ip prefix-list PLIST1 permit 172.20.5.0/24
!
route-map SETLP permit 10
  match ip address prefix-list PLIST1
  set local-preference 90
!
router bgp 111
  neighbor 192.168.10.1 remote-as 100
  neighbor 192.168.10.1 route-map SETLP in
  neighbor 192.168.20.2 remote-as 200
```

AS 111 wanted to use AS 200 as the preferred path for 172.20.5.0/24 and AS 100 as the backup. After the configuration, AS 100 is not used for any other routes. Which configuration resolves the issue?

- A. route-map SETLP permit 10  
match ip address prefix-list PLIST1

set local-preference 110  
route-map SETLP permit 20

B. route-map SETLP permit 10  
match ip address prefix-list PLIST1  
set local-preference 99  
route-map SETLP permit 20

C. router bgp 111  
no neighbor 192.168.10.1 route-map SETLP in  
neighbor 192.168.20.2 route-map SETLP in

D. router bgp 111  
no neighbor 192.169.10.1 route-map SETLP in  
neighbor 192.168.10.1 route-map SETLP out

**Answer: B**

Question (added on 28th-Jul-2021) =====

#### **Question 49**

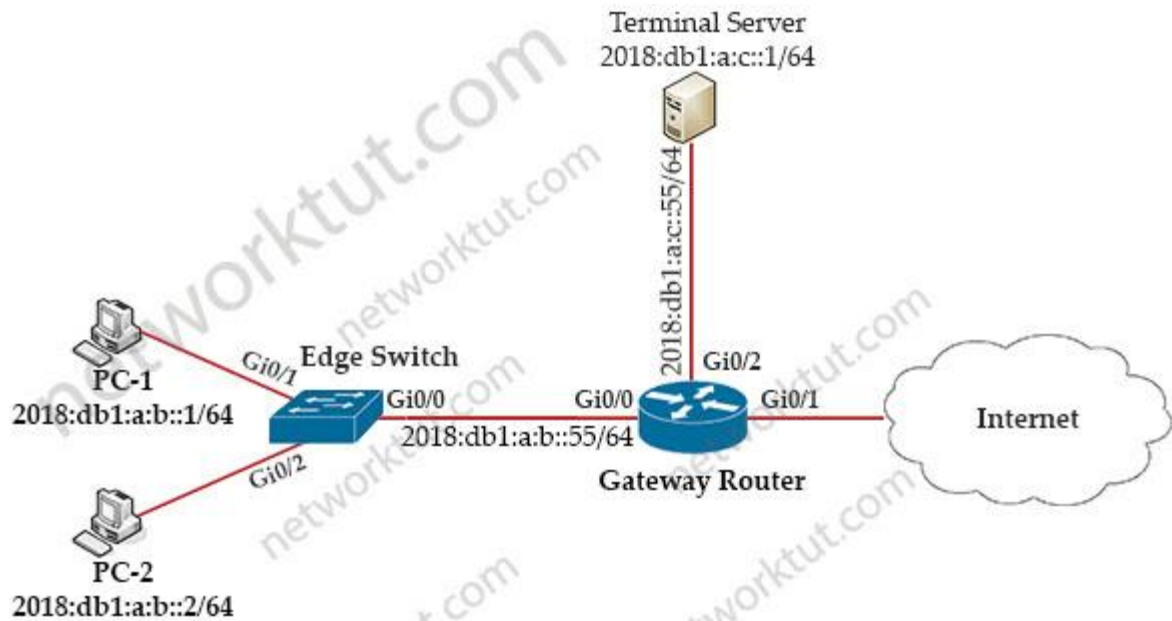
A customer reports to the support desk that they cannot print from their PC to the local printer id:401987778. Which tool must be used to diagnose the issue using Cisco DNA Center Assurance?

- A. application trace
- B. path trace
- C. ACL trace
- D. device trace

**Answer: B**

#### **Question 50**

Refer to the exhibit.



```
Gateway-Router# show ipv6 access-list
IPv6 access list Default_Access
permit tcp host 2018:DB1:A:B::1 host 2018:DB1:A:C::1 eq www sequence 10
deny tcp any host 2018:DB1:A:C::1 eq telnet sequence 20
permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet sequence 30
permit ipv6 2018:DB1:A:B::/64 any sequence 40
```

PC-2 failed to establish a Telnet connection to the terminal server. Which configuration resolves the issue?

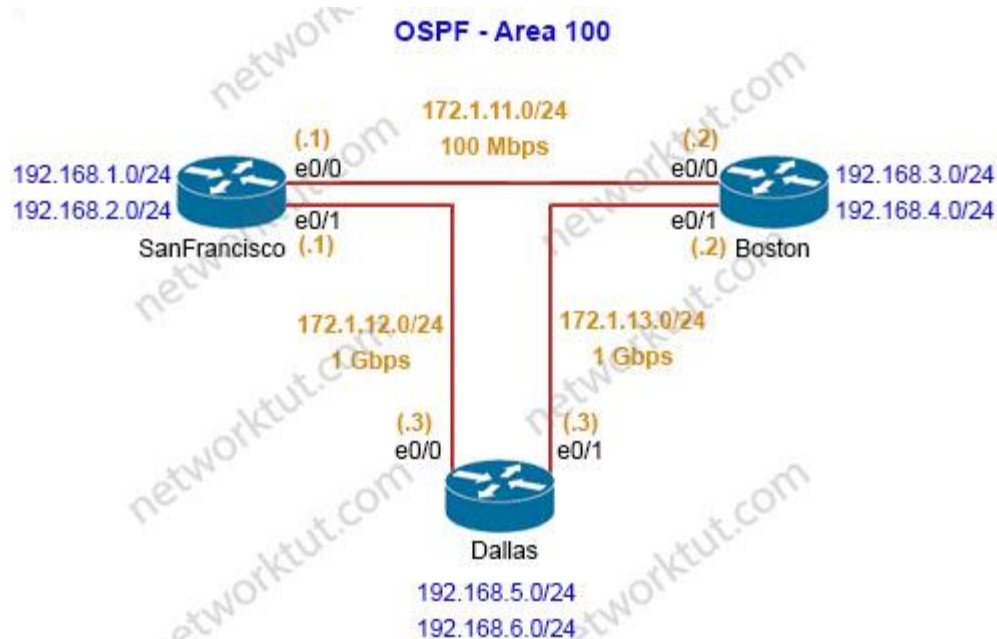
- A. Gateway-Router(config)#ipv6 access-list Default\_Access  
Gateway-Router(config-ipv6-acl)#sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
- B. Gateway-Router(config)#ipv6 access-list Default\_Access  
Gateway-Router(config-ipv6-acl)#permit tcp host 2018:D81:A:B::2 host 2018:DB1:A:C::1 eq telnet
- C. Gateway-Router(config)#ipv6 access-list Default\_Access  
Gateway-Router(config-ipv6-acl)#no sequence 20  
Gateway-Router(config-ipv6-acl)#sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
- D. Gateway-Router(config)#ipv6 access-list Default\_Access  
Gateway-Router(config-ipv6-acl)#sequence 25 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet

**Answer: A**



## Question 51

Refer to the exhibit.



### Show IP Route - San Francisco Router

Gateway of last resort is not set

```
172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
C   172.1.11.0/24 is directly connected, Ethernet0/0
L   172.1.11.1/32 is directly connected, Ethernet0/0
C   172.1.12.0/24 is directly connected, Ethernet0/1
L   172.1.12.1/32 is directly connected, Ethernet0/1
O   172.1.13.0/24 [110/11] via 172.1.11.2, 00:02:34, Ethernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, Loopback0
L   192.168.1.1/32 is directly connected, Loopback0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.2.0/24 is directly connected, Loopback1
L   192.168.2.1/32 is directly connected, Loopback1
O   192.168.3.0/24 [110/11] via 172.1.11.2, 00:00:44, Ethernet0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.2.0/24 is directly connected, Loopback1
L   192.168.2.1/32 is directly connected, Loopback1
O   192.168.3.0/24 [110/11] via 172.1.11.2, 00:00:44, Ethernet0/0
O   192.168.4.0/24 [110/11] via 172.1.11.2, 00:00:34, Ethernet0/0
O   192.168.5.0/24 [110/11] via 172.1.12.3, 00:00:34, Ethernet0/1
O   192.168.6.0/24 [110/11] via 172.1.12.3, 00:00:24, Ethernet0/1
```

### Show IP Route - Boston

Gateway of last resort is not set

```
172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
O   172.1.11.0/24 [110/11] via 172.1.13.2, 00:04:44, Ethernet0/1
    [110/11] via 172.1.12.1, 00:04:44, Ethernet0/0
C   172.1.12.0/24 is directly connected, Ethernet0/0
L   172.1.12.3/32 is directly connected, Ethernet0/0
C   172.1.13.0/24 is directly connected, Ethernet0/1
L   172.1.13.3/32 is directly connected, Ethernet0/1
O   192.168.1.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
```

```

O    192.168.2.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/1
O    192.168.3.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
O    192.168.4.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
    192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.5.0/24 is directly connected, Loopback0
L    192.168.5.1/32 is directly connected, Loopback0
    192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.6.0/24 is directly connected, Loopback1
L    192.168.6.1/32 is directly connected, Loopback1

```

SanFrancisco and Boston routers are choosing slower links to reach each other despite the direct links being up. Which configuration fixes the issue?

<b>Option A</b>  All Routers router ospf 1 auto-cost reference-bandwidth 100	<b>Option B</b>  Boston Router router ospf 1 auto-cost reference-bandwidth 1000
<b>Option C</b>  All Routers router ospf 1 auto-cost reference-bandwidth 1000	<b>Option D</b>  SanFrancisco Router router ospf 1 auto-cost reference-bandwidth 1000

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

## Question 52

Drag and drop the LDP features from the left onto the descriptions on the right.

explicit null label	packet is encapsulated in MPLS with the option of copying the IP precedence to EXP bits
inbound label binding filtering	provides ways of improving load balancing by eliminating the need for DPI at transit LSRs
implicit null label	LSR receives an MPLS header with the label set to 3
entropy label	controls the amount of memory used to store LDP label bindings advertised by other devices

**Answer:**

- + packet is encapsulated in MPLS with the option of copying the IP precedence to EXP bits: explicit null label
- + provides ways of improving load balancing by eliminating the need for DPI at transit LSRs: entropy label
- + LSR receives an MPLS header with the label set to 3: implicit null label
- + controls the amount of memory used to store LDP label bindings advertised by other devices: inbound label binding filtering

**Question 53**

Refer to the exhibit.

Debug output:

```
username: USER55
password:
Aug 26 12:39:23.813: TPLUS: Queuing AAA Authentication request 4950 for
processing
Aug 26 12:39:23.813: TPLUS(00001356) login timer started 1020 sec timeout
Aug 26 12:39:23.813: TPLUS: processing authentication continue request id
4950
Aug 26 12:39:23.813: TPLUS: Authentication continue packet generated for 4950
Aug 26 12:39:23.813: TPLUS(00001356)/0/WRITE/3A72C8D0: Started 5 sec timeout
!
!---output omitted---!
!
Aug 26 12:40:01.241: TAC+: using previously set server 192.168.1.3 from group
tacacs+
Aug 26 12:40:01.241: TAC+: Opening TCP/IP to 192.168.1.3/49 timeout=5
Aug 26 12:40:01.249: TAC+: Opened TCP/IP handle 0x3BE31D1C to 192.168.1.3/49
Aug 26 12:40:01.249: TAC+: Opened 192.168.1.3 index=1
Aug 26 12:40:01.250: TAC+: 192.168.1 3 (3653537180) AUTHOR/START queued
Aug 26 12:40:01.449: TAC+: (3653537180) AUTHOR/START processed
Aug 26 12:40:01.449: TAC+: (-641430116): received author response status =
FAIL
Aug 26 12:40:01.450. TAC+: Closing TCP/IP 0x3BE31D1C connection to
192.168.1.3/49
```

A network administrator logs into the router using TACACS+ username and password credentials, but the administrator cannot run any privileged commands. Which action resolves the issue?

- A. Configure TACACS+ synchronization with the Active Directory admin group
- B. Configure the username from a local database
- C. Configure full access for the username from TACACS+ server
- D. Configure an authorized IP address for this user to access this router

**Answer: C**

**Question 54**

How does an MPLS Layer 3 VPN function?

- A. set of sites use multiprotocol BGP at the customer site for aggregation
- B. multiple customer sites interconnect through a service provider network using customer edge to provider edge connectivity
- C. set of sites interconnect privately over the Internet for security
- D. multiple customer sites interconnect through service provider network to create secure tunnels between customer edge devices

**Answer: B**

### Question 55

Refer to the exhibit.

```
ipv6 access-list INTERNET
 permit ipv6 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA14::/64
 permit tcp 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA13::/64 eq telnet
 permit tcp 2001:DB8:AD59:BA21::/64 any eq http
 permit ipv6 2001:DB8:AD59::/48 any
 deny ipv6 any any log
```

While monitoring VTY access to a router, an engineer notices that the router does not have any filter and anyone can access the router with username and password even through the ACL is configured. Which command resolves this issue?

- A. ipv6 traffic-filter INTERNET in
- B. access-class INTERNET in
- C. ipv6 access-class INTERNET in
- D. ip access-group INTERNET in

**Answer: C**

### Question 56

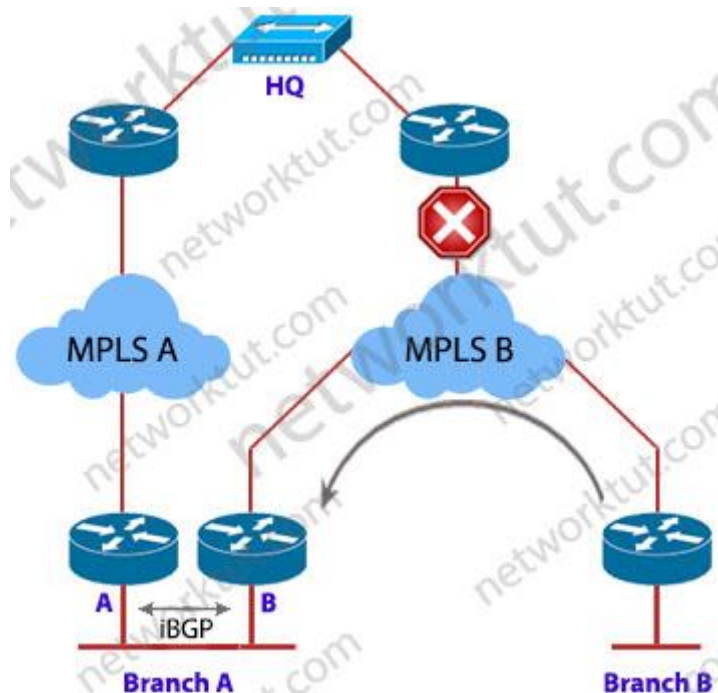
An engineer configured Reverse Path Forwarding on an interface and noticed that the routes are dropped when a route lookup fails on that interface for a prefix that is available in the routing table. Which interface configuration resolves the issue?

- A. ip verify unicast source reachable-via rx
- B. ip verify unicast source reachable-via any
- C. ip verify unicast source reachable-via allow-default
- D. ip verify unicast source reachable-via 12-src

**Answer: B**

### Question 57

Refer to the exhibit.



Troubleshoot and ensure that branch B only ever uses the MPLS B network to reach HQ. Which action achieves this requirement?

- A. Modify the weight of all HQ prefixes received at branch B from the MPLS B network to be higher than the weights used on the MPLS A network
- B. Increase the local preference for all HQ prefixes received at branch B from the MPLS B network to be higher than the local preferences used on the MPLS A network
- C. Introduce AS path prepending on the branch A MPLS B network connection so that any HQ advertisements from branch A toward the MPLS B network are prepended three times
- D. Introduce an AS path filter on branch A routers so that only local prefixes are advertised into BGP

**Answer: D**

### Question 58

Refer to the exhibit.

```
LA
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
NY
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
```

```
!  
interface E0/0  
  ip ospf authentication message-digest  
  ip ospf message-digest-key 1 md5 Cisco123
```

The neighbor relationship is not coming up. Which two configurations bring the adjacency up?  
(Choose two)

A. LA

```
router ospf 1  
area 0 authentication message-digest
```

B. NY

```
interface E0/0  
no ip ospf message-digest-key 1 md5 Cisco123  
ip ospf authentication-key Cisco123
```

C. LA

```
interface E0/0  
ip ospf authentication-key Cisco123
```

D. LA

```
interface E0/0  
ip ospf message-digest-key 1 md5 Cisco123
```

E. NY

```
router ospf 1  
area 0 authentication message-digest
```

**Answer: A D**

## Question 59

Refer to the exhibit.

```
router ospf 1  
  redistribute eigrp 1 subnets route-map EIGRP->OSPF  
!  
router eigrp 1  
  network 10.0.106.0 0.0.0.255  
!  
route-map EIGRP->OSPF permit 10  
  match ip address WAN_PREFIXES  
route-map EIGRP->OSPF permit 20  
  match ip address LOCAL_PREFIXES  
route-map EIGRP->OSPF permit 30  
  match ip address VPN_PREFIXES  
!  
ip prefix-list LOCAL_PREFIXES seq 5 permit 172.16.0.0/12 le 24  
ip prefix-list VPN_PREFIXES seq 5 permit 192.168.0.0/16 le 24  
ip prefix-list WAN_PREFIXES seq 5 permit 10.0.0.0/8 le 24  
!
```

The network administrator configured redistribution on an ASBR to reach to all WAN networks but failed. Which action resolves the issue?

- A. The route map must have the keyword prefix-list to evaluate the prefix list entries
- B. The OSPF process must have a metric when redistributing prefixes from EIGRP
- C. The route map EIGRP->OSPF must have the 10.0.106.0/24 entry to exist in one of the three prefix lists to pass
- D. EIGRP must redistribute the 10.0.106.0/24 route instead of using the network statement

**Answer: A**

### Question 60

Refer to the exhibit.

#### Configuration Output

```
aaa new-model
!
aaa authentication login default local
aaa authentication login VTY_AUTH local
aaa authorization exec default none
aaa authorization exec VTY_AUTH local
aaa accounting exec default start-stop group radius
!
```

```
password 7 KQAYUutfDrf0g04s
authorization exec VTY_AUTH
login authentication VTY_AUTH
```

```
!
```

#### Debug Output:

```
AAA/AUTHEN/LOGIN (000004B6): Pick method list 'default'
AAA/AUTHOR (0x486): Pick method list 'VTY_AUTH'
AAA/AUTHOR/EXEC(000004B6): Authorization FAILED
```

Which action resolves the failed authentication attempt to the router?

- A. Configure **aaa authorization login** command on line vty 0 4
- B. Configure **aaa authorization login** command on line console 0
- C. Configure **aaa authorization console** global command
- D. Configure **aaa authorization console** command on line vty 0 4

**Answer: C**

## Question 61

Refer to the exhibit.

```
Router# show ip route
```

```
    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
```

```
Router# show ip bgp
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 2.2.2.0/24	0.0.0.0	0	32768	?	
*> 131.108.1.0/24	2.2.2.2	84	32768	?	
*> 131.108.2.0/24	2.2.2.2	74	32768	?	

The OSPF routing protocol is redistributed into the BGP routing protocol, but not all the OSPF routes are distributed into BGP. Which action resolves the issue?

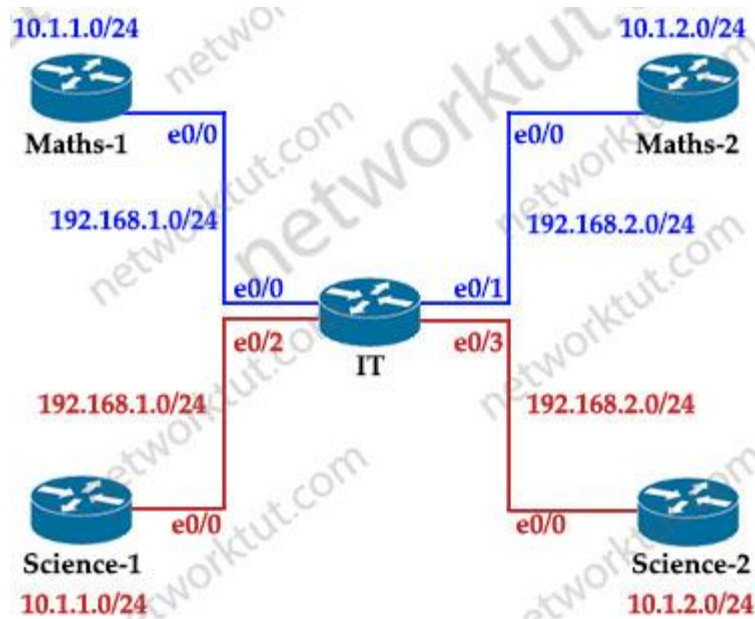
- A. Use a route-map command to redistribute OSPF external routes defined in a prefix list.
- B. Use a route-map command to redistribute OSPF external routes defined in an access list
- C. Include the word **external** in the redistribute command
- D. Include the word **internal external** in the redistribute command

**Answer: D**

## Question 62

Refer to the exhibit.





The Math and Science departments connect through the corporate IT router but users in the Math department must not be able to reach the Science department and vice versa. Which configuration accomplishes this task?

#### Option A

```
vrf definition Science
address-family ipv4
!
interface E0/2
ip address 192.168.1.1 255.255.255.0
no shut
!
interface E0/3
ip address 192.168.2.1 255.255.255.0
no shut
!
```

#### Option B

```
vrf definition Science
!
interface E0/2
ip address 192.168.1.1 255.255.255.0
no shut
!
interface E0/3
ip address 192.168.2.1 255.255.255.0
no shut
```

#### Option C

```
vrf definition Science
address-family ipv4
!
interface E0/2
vrf forwarding Science
ip address 192.168.1.1 255.255.255.0
no shut
!
interface E0/3
vrf forwarding Science
ip address 192.168.2.1 255.255.255.0
no shut
```

#### Option D

```
vrf definition Science
address-family ipv4
!
interface E0/2
ip address 192.168.1.1 255.255.255.0
vrf forwarding Science
no shut
!
interface E0/3
ip address 192.168.2.1 255.255.255.0
vrf forwarding Science
no shut
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

### Question 63

When determining if a system is capable of support, what is the minimum time spacing required for a BFD control packet to receive once a control packet is arrived?

- A. Desired Min TX Interval
- B. Detect Mult
- C. Required Min RX Interval
- D. Required Min Echo RX Interval

**Answer: C**

### Question 64

While troubleshooting an EIGRP neighbor adjacency problem, the network engineer notices that the interface connected to the neighboring router is not participating in the EIGRP process. Which action resolves the issues?

#### EIGRP-IPv4 Interfaces for AS(10)

Interface	Xmit Queue	Mean	Pacing Time	Multicast		
	Peers	Un/Reliable	SRTT	Un/Reliable	Flow	
Lo0	0	0/0	0	0/0	0	
Fa0/0	1	0/0	7	0/2	50	0

Router#show running-config | section eigrp

router eigrp 1

network 172.16.0.0 0.0.0.255

network 192.168.2.2 0.0.0.0

network 192.168.12.2 0.0.0.0

Router#show running-config interface Fa0/3

Building configuration...

Current configuration: 93 bytes

!

interface FastEthernet0/3

ip vrf forwarding CLIENT1

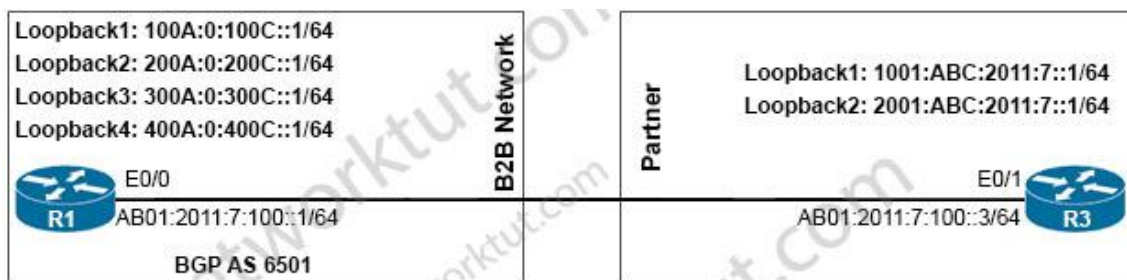
ip address 172.16.0.1 255.255.255.0

- A. Configure the network command to network 172.16.0.1 0.0.0.0
- B. Configure the network command under EIGRP address family vrf CLIENT1
- C. Configure EIGRP metrics on interface FastEthernet0/3
- D. Configure the network command under EIGRP address family ipv4

**Answer: B**

### Question 65

Refer to the exhibit. An engineer configured BGP between routers R1 and R3. The BGP peers cannot establish neighbor adjacency to be able to exchange routes. Which configuration resolves this issue?



R1#sh bgp ipv6 sum

BGP router identifier 1.1.1.1, local AS number 6501

BGP table version is 1, main routing table version 1

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
AB01:2011:7:100::3	4	6502	0	0	1	0	0	never	Idle

R1#debug ip bgp all

```
* Nov 8 17:22:11.223: BGP: AB01:2011:7:100::3 active went from Idle to Active
* Nov 8 17:22:11.223: BGP: AB01:2011:7:100::3 open active, local address AB01:2011:7:100::1
* Nov 8 17:22:11.224: BGP: AB01:2011:7:100::3 open failed: Connection refused by remote host
* Nov 8 17:22:11.224: BGP: AB01:2011:7:100::3 Active open failed - tcb is not available, open
active delayed 11264 ms (35000ms max, 60% jitter)
* Nov 8 17:22:11.224: BGP: ses global AB01:2011:7:100::3 (0xC3F49FF0:0) act Reset (Active open failed)
* Nov 8 17:22:11.232: BGP: AB01:2011:7:100::3 active went from Active to Idle
* Nov 8 17:22:11.232: BGP: nrb global AB01:2011:7:100::3 Active open failed - open timer running
```

R1#ping ipv6 AB01:2011:7:100::3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to AB01:2011:7:100::3, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

#### Option A

R1  
 router bgp 6501  
 address-family ipv6  
 neighbor AB01:2011:7:100::3 activate

#### Option B

R3  
 router bgp 6502  
 address-family ipv6  
 neighbor AB01:2011:7:100::1 activate

**Option C**

```
R1
router bgp 6501
neighbor AB01:2011:7:100::3 ebgp-multihop
255
```

**Option D**

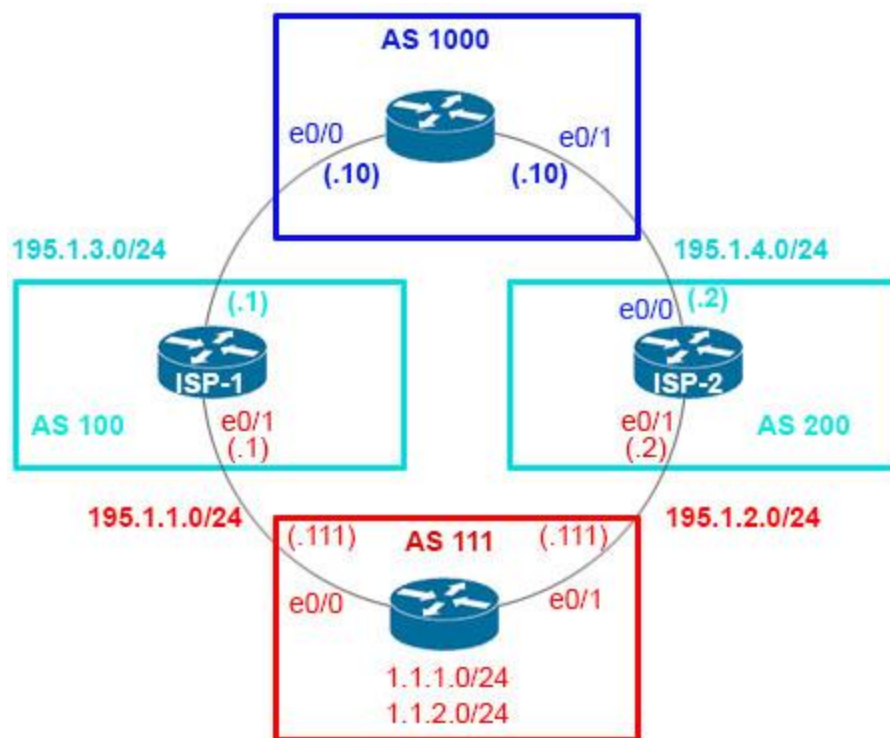
```
R3
router bgp 6502
neighbor AB01:2011:7:100::1 ebgp-multihop
255
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

**Question 66**

Refer to the exhibit.

**AS111**

```
router bgp 111
neighbor 195.1.1.1 remote-as 100
neighbor 195.1.1.1 allowas-in
neighbor 195.1.2.2 remote-as 200
neighbor 195.1.2.2 allowas-in
```

AS111 is receiving its own routes from AS200 causing a loop in the network. Which configuration provides loop prevention?

<b>Option A</b>  router bgp 111 neighbor 195.1.1.1 as-override neighbor 195.1.2.2 allowas-in	<b>Option B</b>  router bgp 111 neighbor 195.1.2.2 as-override no neighbor 195.1.1.1 allowas-in
<b>Option C</b>  router bgp 111 neighbor 195.1.1.1 as-override neighbor 195.1.2.2 as-override	<b>Option D</b>  router bgp 111 no neighbor 195.1.1.1 allowas-in no neighbor 195.1.2.2 allowas-in

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

#### **Question 67**

Which mechanism must be chosen to optimize the reconvergence time for OSPF at company location 407553457 that is less CPU-intensive than reducing the hello and dead timers?

- A. SSO
- B. OSPF demand circuit
- C. Dead Peer Detection keepalives
- D. BFD

**Answer: D**

#### **Question 68**

Refer to the exhibit. Which set of commands restore reachability to loopback0?

```

interface loopback0
ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet1/0
Description *** WAN link ***
ip address 10.0.0.1 255.255.255.0
!
interface FastEthernet1/1
Description *** LAN Network ***
ip address 192.168.1.1 255.255.255.0
!
!
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 4.4.4.4 0.0.0.0 area 0
network 10.0.0.1 0.0.0.0 area 0
network 192.168.1.1 0.0.0.0 area 10
!

```

A. interface loopback0  
ip address 4.4.4.4 255.255.255.0  
ip ospf network point-to-point

B. interface loopback0  
ip address 4.4.4.4 255.255.255.0  
ip ospf interface area 10

C. interface loopback0  
ip address 4.4.4.4 255.255.255.0  
ip ospf interface type network

D. interface loopback0  
ip address 4.4.4.4 255.255.255.0  
ip ospf network broadcast

**Answer: A**

### Question 69

Refer to the exhibit.

```

Branch-Router#
*Nov 29 15:20:22.415: OSPF-1 HELLO Fa1/1: Rcv hello from 3.3.3 3 area 1 10.2.1.3
*Nov 29 15:20:23.195: OSPF-1 HELLO Fa1/1: Send hello to 224.0.0.5 area 1 from 10.2.1.1

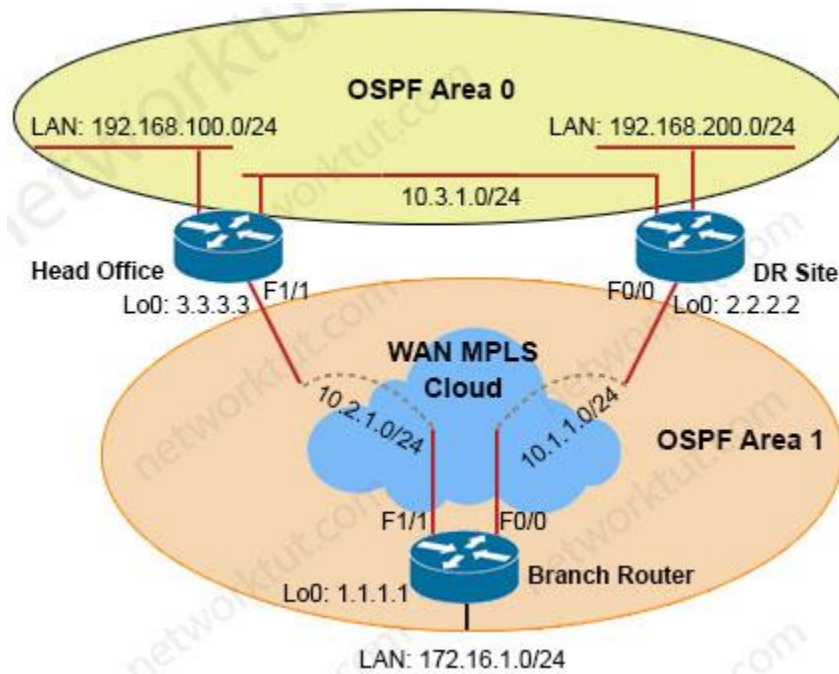
Branch-Router#
*Nov 29 15:20:27.955: OSPF-1 HELLO Fa0/0: Rcv hello from 2.2.2 2 area 1 10.1.1.2

```

```

*Nov 29 15:20:27.955: OSPF-1 HELLO Fa0/0: Mismatched hello parameters from 10.1.1.2
*Nov 29 15:20:27.955: OSPF-1 HELLO Fa0/0: Dead R 40 C 40, Hello R 10 C 10 Mask R
255.255.255.0 C 255.255.255.240
*Nov 29 15:20:28.311: OSPF-1 HELLO Fa0/0: Send hello to 224.0.0.5 area 1 from 10.1.1.1

```



A network administrator reviews the branch router console log to troubleshoot the OSPF adjacency issue with the DR router. Which action resolves this issue?

- A. Stabilize the DR site flapping link to establish OSPF adjacency
- B. Configure matching hello and dead intervals between sites
- C. Advertise the branch WAN interface matching subnet for the DR site
- D. Configure the WAN interface for DR site in the related OSPF area

**Answer: C**

### Question 70

A network administrator performed a Compact Flash Memory upgrade on a Cisco Catalyst 6509 Switch. Everything is functioning normally except SNMP, which was configured to monitor the bandwidth of key interfaces but the interface indexes are changed. Which global configuration resolves the issue?

- A. snmp-server ifindex persist
- B. snmp-server ifindex permanent
- C. snmp ifindex permanent
- D. snmp ifindex persist

**Answer: A**

### Question 71

How is VPN routing information distributed in an MPLS network?

- A. It is established using VPN IPsec peers.
- B. It is controlled through the use of RD
- C. The top level of the customer data packet directs it to the correct CE device
- D. It is controlled using of VPN target communities

**Answer: D**

### Question 72

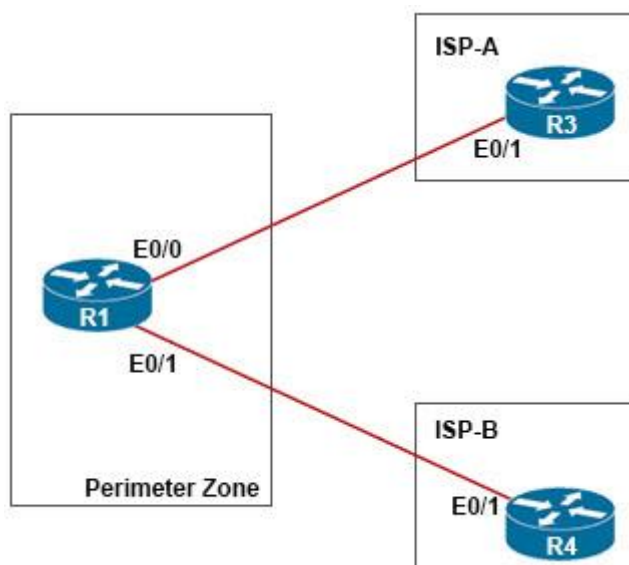
Users report issues with reachability between areas as soon as an engineer configured summary routes between areas in a multiple area OSPF autonomous system. Which action resolves the issue?

- A. Configure the **summary-address** command on the ABR
- B. Configure the **area range** command on the ASBR
- C. Configure the **summary-address** command on the ASBR
- D. Configure the **area range** command on the ABR

**Answer: D**

### Question 73

Refer to the exhibit.





A network is under a cyberattack. A network engineer connected to R1 by SSH and enabled the terminal monitor via SSH session to find the source and destination of the attack. The session was flooded with messages, which made it impossible for the engineer to troubleshoot the issue. Which command resolves this issue on R1?

- A. #terminal no monitor
- B. #no terminal monitor
- C. (config)#no terminal monitor
- D. (config)#terminal no monitor

**Answer: A**

### Question 74

Refer to the exhibit.



Which action resolves the adjacency issue?

- A. Match the hello interval timers
- B. Match the authentication keys
- C. Configure the same EIGRP process IDs
- D. Configure the same autonomous system numbers

**Answer: D**

### Question 75

Refer to the exhibit.

```
admin@linux:~$ scp script.py admin@198.51.100.64:script.py
```

```
Password:
Administratively disabled.
admin@linux:~$ Connection to 198.51.100.64 closed by remote host.
```

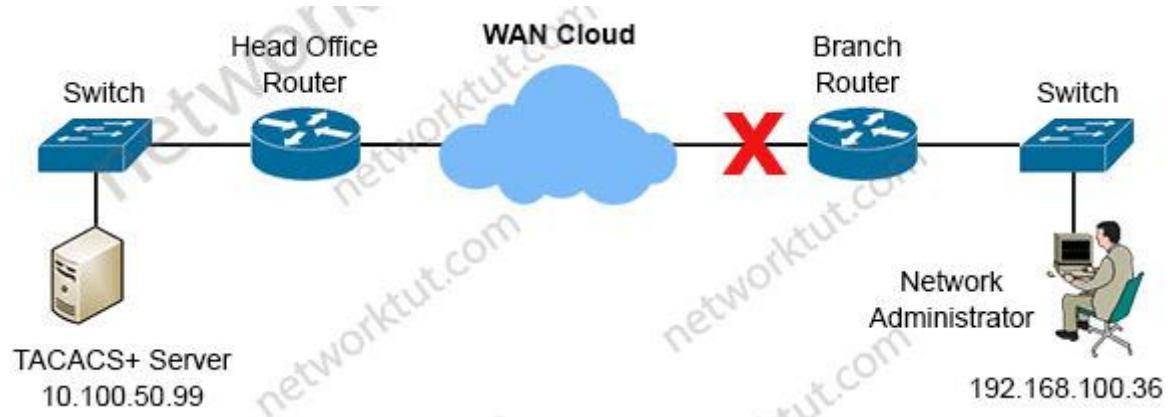
A network administrator has developed a Python script on the local Linux machine and is trying to transfer it to the router. However, the transfer fails. Which action resolves this issue?

- A. The Python interpreter must first be enabled with the **guestshell enable** command
- B. The SSH service must be enabled with the **crypto key generate rsa** command
- C. The SSH access must be allowed on the VTY lines using the **transport input ssh** command
- D. The SCP service must be enabled with the **ip scp server enable** command

**Answer: D**

### Question 76

Refer to the exhibit.



A network administrator is trying to access a branch router using TACACS+ username and password credentials, but the administrator cannot log in to the router because the WAN connectivity is down. The branch router has following AAA configuration:

```
aaa new-model
aaa authorization commands 15 default group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
tacacs-server host 10.100.50.99
tacacs-server key Ci$co123
```

Which command will resolve this problem when WAN connectivity is down?

- A. `aaa authentication login default group tacacs+ enable`
- B. `aaa authentication login console group tacacs+ enable`

- C. aaa authentication login default group tacacs+ console
- D. aaa authentication login default group tacacs+ local

**Answer: D**

### Question 77

IPv6 is enabled in the infrastructure to support customers with an IPv6 network over WAN and to connect the head office to branch offices in the local network. One of the customers is already running IPv6 and wants to enable IPv6 over the DMVPN network infrastructure between the headend and branch sites. Which configuration command must be applied to establish an mGRE IPv6 tunnel neighborship?

- A. ipv6 nhrp holdtime 30
- B. ipv6 unicast-routing
- C. tunnel mode gre multipoint ipv6
- D. tunnel protection mode ipv6

**Answer: C**

### Question 78

Refer to the exhibit.



An engineer configured SNMP communities on the Core\_Sw1, but the SNMP server cannot obtain information from Core\_Sw1. Which configuration resolves this issue?

- A. access-list 20 permit 10.221.10.12
- B. snmp-server group NETVIEW v2c priv read NETVIEW access 20

- C. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22  
D. access-list 20 permit 10.221.10.11

**Answer: D**

### Question 79

Refer to the exhibit.

```
P 172.29.0.0/16, 1 successors, FD is 307200, serno 2
  via 192.168.254.2 (307200/281600), FastEthernet0/1
  via 192.168.253.2 (410200/352300), FastEthernet0/0
```

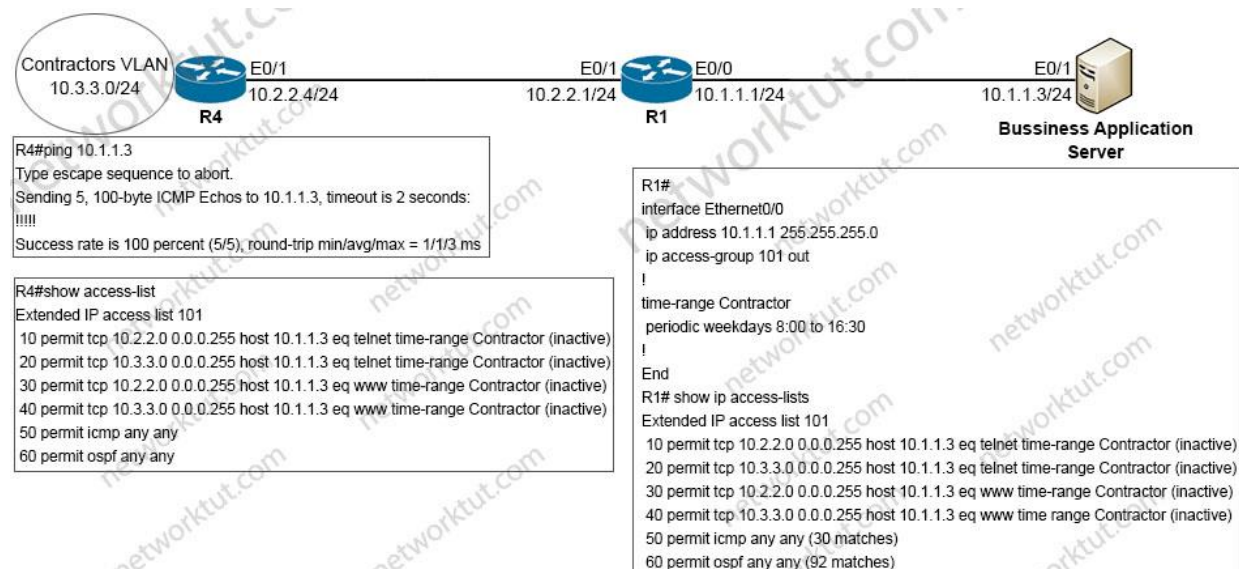
When the FastEthernet0/1 goes down, the route to 172.29.0.0/16 via 192.168.253.2 is not installed in the RIB. Which action resolves the issue?

- A. Configure reported distance greater than the feasible distance
- B. Configure feasible distance greater than the successor's feasible distance
- C. Configure feasible distance greater than the reported distance
- D. Configure reported distance greater than the successor's feasible distance

**Answer: C**

### Question 80

Refer to the exhibit.



An engineer is troubleshooting failed access by contractors to the business application server via Telnet or HTTP during the weekend. Which configuration resolves the issue?

A. R4

no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor

B. R1

no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor

C. R4

time-range Contractor

no periodic weekdays 17:00 to 23:59

periodic daily 8:00 to 16:30

D. R1

time-range Contractor

no periodic weekdays 8:00 to 16:30

periodic daily 8:00 to 16:30

**Answer: D**

### Question 81

Refer to the exhibit.

```
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
```

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?

A. It is sent to 209.165.202.129.

B. It is sent to 209.165.202.131.

C. It is forwarded using the routing table lookup.

D. It is dropped.

**Answer: B**

### Question 82

Refer to the exhibit.

```
*Sep 26 19:50:43.504: SNMP: Packet received via UDP from  
192.168.1.2 on GigabitEthernet0/1SrParseV3SnmpMessage: No matching Engine ID.
```

```
SrParseV3SnmpMessage: Failed.  
SrDoSnmp: authentication failure, Unknown Engine ID
```

```
*Sep 26 19:50:43.504: SNMP: Report, reqid 29548, errstat 0,  
erridx 0  
internet.6.3.15.1.1.4.0 = 3  
*Sep 26 19:50:43.508: SNMP: Packet sent via UDP to 192.168.1.2  
process_mgmt_req_int: UDP packet being de-queued
```

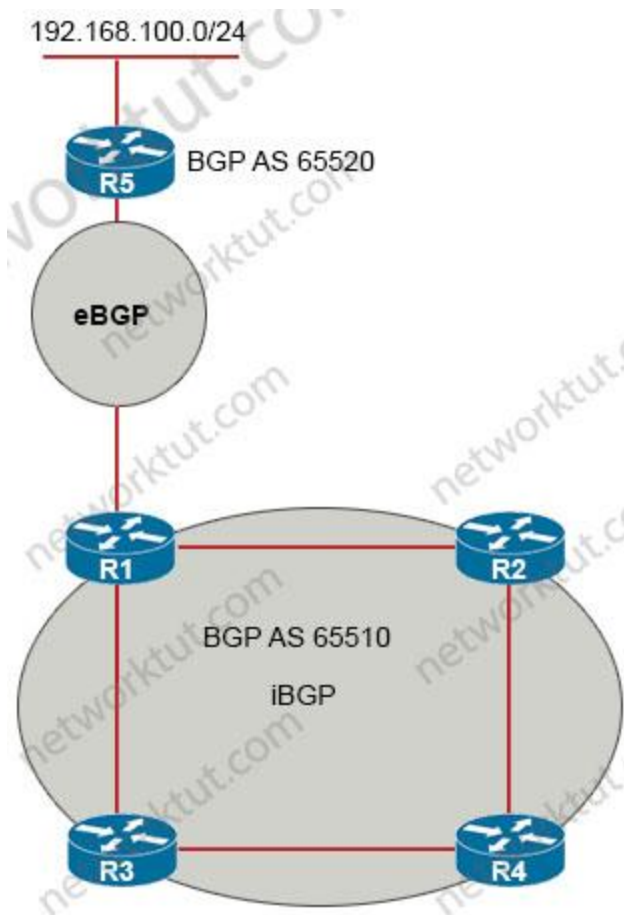
Which two commands provide the administrator with the information needed to resolve the issue? (Choose two)

- A. show snmp user
- B. debug snmp engine-id
- C. show snmpv3 user
- D. debug snmpv3 engine-id
- E. debug snmp packet

**Answer:** A E

### Question 83

Refer to the exhibit.



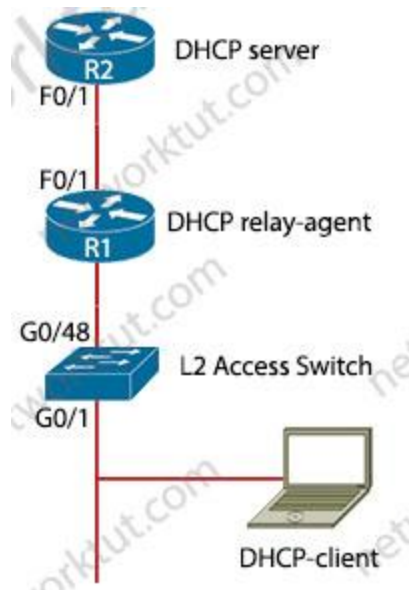
AS65510 iBGP is configured for directly connected neighbors. R4 cannot ping or traceroute network 192.168.100.0/24. Which action resolves this issue?

- A. Configure R1 as a route reflector server and configure R2 and R3 as route reflector clients
- B. Configure R4 as a route reflector server and configure R2 and R3 as route reflector
- C. Configure R4 as a route reflector server and configure R1 as a route reflector client
- D. Configure R1 as a route reflector server and configure R4 as a route reflector client

**Answer: D**

#### **Question 84**

Refer to the exhibit.



The network administrator can see the DHCP discovery packet in R1, but R2 is not replying to the DHCP request. The R1 related interface is configured with the DHCP helper address. If the PC is directly connected to the Fa0/1 interface on R2, the DHCP server assigns as IP address from the DHCP pool to the PC. Which two commands resolve this issue? (Choose two)

- A. ip dhcp relay information trust-all command on R2
- B. ip dhcp relay information enable command on R1
- C. ip dhcp option 82 command on R2
- D. service dhcp-relay command on R1
- E. service dhcp command on R1

**Answer:** A E

### Question 85

A network administrator is troubleshooting a high utilization issue on the route processor of a router that was reported by NMS. The administrator logged into the router to check the control plane policing and observed that the BGP process is dropping a high number of routing packets and causing thousands of routes to recalculate frequently. Which solution resolves this issue?

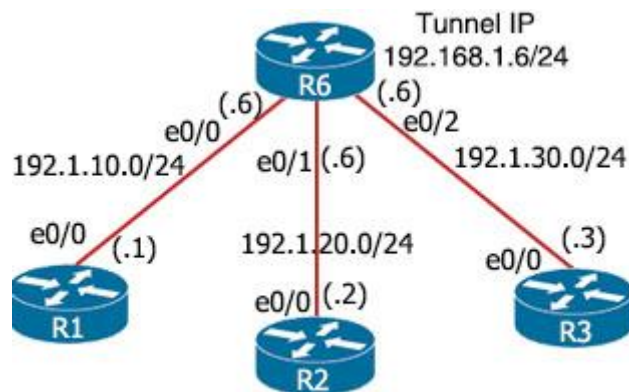
- A. Police the pir for BGP, conform-action set-prec-transmit, and exceed action set-clp-transmit
- B. Police the pir for BGP, conform-action transmit, and exceed action transmit
- C. Shape the cir for BGP, conform-action transmit, and exceed action transmit
- D. Shape the pir for BGP, conform-action set-prec-transmit, and exceed action set-frde-transmit

**Answer:** A

### Question 86



Refer to the exhibit.



An engineer must establish multipoint GRE tunnels between hub router R6 and branch routers R1, R2, and R3. Which configuration accomplishes this task on R1?

<p><b>Option A</b></p> <pre> interface Tunnel 1 ip address 192.168.1.1 255.255.255.0 tunnel source e0/0 tunnel mode gre multipoint ip nhrp nhs 192.168.1.6 ip nhrp map 192.168.1.6 192.1.10.1 ip nhrp map 192.168.1.2 192.1.20.2 ip nhrp map 192.168.1.3 192.1.30.3 </pre>	<p><b>Option B</b></p> <pre> interface Tunnel 1 ip address 192.168.1.1 255.255.255.0 tunnel source e0/1 tunnel mode gre multipoint ip nhrp nhs 192.168.1.6 ip nhrp map 192.168.1.6 192.1.10.6 </pre>
<p><b>Option C</b></p> <pre> interface Tunnel 1 ip address 192.168.1.1 255.255.255.0 tunnel source e0/0 tunnel mode gre multipoint ip nhrp network-id 1 ip nhrp nhs 192.168.1.6 ip nhrp map 192.168.1.6 192.1.10.6 </pre>	<p><b>Option D</b></p> <pre> interface Tunnel 1 ip address 192.168.1.1 255.255.255.0 tunnel source e0/1 tunnel mode gre multipoint ip nhrp network-id 1 ip nhrp nhs 192.168.1.6 ip nhrp map 192.168.1.6 192.1.10.1 ip nhrp map 192.168.1.2 192.1.20.2 ip nhrp map 192.168.1.3 192.1.30.3 </pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

# New ENARSI Questions 2

## Question 1

An engineer configured SNMP notifications sent to the management server using authentication and encryption data with DES. An error in the response PDU is received as “UNKNOWNUSERNAME, WRONGDIGEST”. Which action resolves the issue?

- A. Configure correct authentication and privacy passwords using SNMPv3 authNoPriv
- B. Configure the correct authentication password using SNMPv3 authPriv
- C. Configure the correct authentication password using SNMPv3 authNoPriv
- D. Configure correct authentication and privacy passwords using SNMPv3 authPriv

**Answer:** B or D

## Question 2

An engineer configured a cisco router to send reliable and encrypted notifications for any events to the management server. It was noticed that line notifications messages are reliable but not encrypted. Which action resolves the issue?

- A. Configure all devices for SNMPv3 traps with priv
- B. Configure all devices for SNMPv3 informs with auth
- C. Configure all devices for SNMPv3 informs with priv
- D. Configure all devices for SNMPv3 traps with auth

**Answer:** C

## Question 3

Refer to the exhibit.



The network administrator must mutually redistribute routes at the Chicago router to the LA and NewYork routers. The configuration of the Chicago router is this:

```
router ospf 1
 redistribute eigrp 100
router eigrp 100
 redistribute ospf 1
```

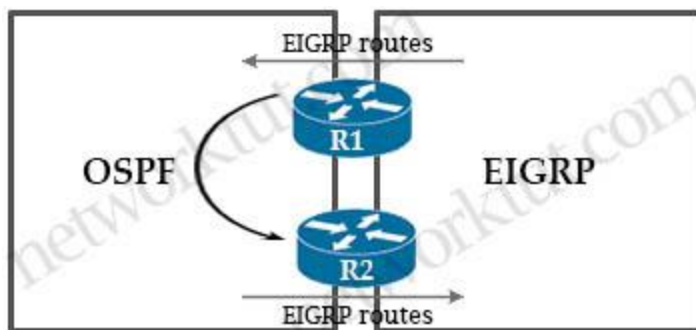
After the configuration, the LA router receives all the NewYork routes, but NewYork router does not receive any LA routes. Which set of configurations fixes the problem on the Chicago router?

- A. router ospf 1  
redistribute eigrp 100 subnets
- B. router eigrp 100  
redistribute ospf 1 metric 10 10 10 10 10
- C. router ospf 1  
redistribute eigrp 100 metric 20
- D. router eigrp 100  
redistribute ospf 1 subnets

**Answer: B**

#### Question 4

Refer to the exhibit.



A network administrator configured mutual redistribution on R1 and R2 routers, which caused instability in the network. Which action resolves the issue?

- A. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to allow when redistributing OSPF into EIGRP.
- B. Set a tag in the route map when redistributing EIGRP into OSPF on R1, and match the same tag on R2 to deny when redistributing OSPF into EIGRP.
- C. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.
- D. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.

**Answer: B**

### Question 5

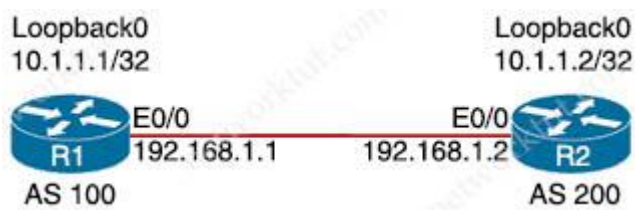
How are MPLS layer 3 VPN services deployed?

- A. The RD and RT values must match under the VRF
- B. The RD and RT values under a VRF must match on the remote PE router
- C. The import and export RT values under a VRF must always be the same
- D. The label switch path must be available between the local and remote PE routers

**Answer: D**

### Question 6

Refer to the exhibit.



<b>R1</b> router bgp 100 neighbor 10.1.1.2 remote-as 200	<b>R2</b> router bgp 200 neighbor 10.1.1.1 remote-as 100
--	--

The neighbor relationship is not coming up. Which two sets of configurations bring the neighbors up? (Choose two)

- A. R2  
ip route 10.1.1.2 255.255.255.255 192.168.1.2  
router bgp 100  
neighbor 10.1.1.2 ttl-security hops 1  
neighbor 10.1.1.2 update-source loopback 0
- B. R1  
ip route 10.1.1.2 255.255.255.255 192.168.1.2  
router bgp 100  
neighbor 10.1.1.2 disable-connected-check  
neighbor 10.1.1.2 update-source loopback0
- C. R2  
ip route 10.1.1.1 255.255.255.255 192.168.1.1  
router bgp 200  
neighbor 10.1.1.1 disable-connected-check  
neighbor 10.1.1.1 update-source loopback0

D. R2

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
router bgp 200
neighbor 10.1.1.1 ttl-security hops 1
neighbor 10.1.1.1 update-source loopback 0
```

**Answer: B C**

### Question 7

What are two functions of IPv6 source guard? (Choose two)

- A. It works independent from IPv6 neighbor discovery
- B. It denies traffic from unknown sources or unallocated addresses
- C. It blocks certain traffic by inspecting DHCP packets for specific sources
- D. It uses the populated binding table for allowing legitimate traffic
- E. It denies traffic by inspecting neighbor discovery packets for specific patterns

**Answer: B D**

### Question 8

An engineer configured access list NON-CISCO in a policy to influence routes.

```
route-map PBR, deny, sequence 5
  Match clauses:
    ip address (access-list): NON-CISCO
  Set clauses:
Policy routing matches: 0 packets, 0 bytes
route-map PBR, permit, sequence 10
  Match clauses:
  Set clauses:
    ip next-hop 192.168.1.5
Policy routing matches: 389202995 packets, 222006352077 bytes
```

What are the two effects of this route map configuration? (Choose two)

- A. Packets are dropped by the access list
- B. Packets are forwarded using normal route lookup
- C. Packets are forwarded to the default gateway
- D. Packets are not evaluated by sequence 10
- E. Packets are evaluated by sequence 10

**Answer: C E**

### Question 9

Refer to the exhibit. All the serial links between R1, R2, and R3 have the same bandwidth. Users on 192.168.1.0/24 (R1) network report slow responses on network 192.168.3.0/24 (R3). A traceroute is run on the path, it shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 are up. What can the network administrator do to fix the slowness.

Note. there is a static route that is making the traffic go the way it currently is.

- A. Change the administrative distance of eigrp to 5
- B. Remove the static route on R1
- C. Add a static route on R1 using the next hop of R3
- D. Redistribute the R1 static route to EIGRP

**Answer: B**

### **Question 10**

Refer to the exhibit.

```
login block-for 15 attempts 10 within 120
login on-failure log
login on-success log
archive
log config
logging enable
logging size 300
notify syslog
snmp-server enable traps syslog
snmp-server host 172.16.17.1 public syslog
```

The administrator can see the traps for the failed login attempts, but cannot see the traps of successful login attempts. What command is needed to resolve the issue?

- A. Configure logging history 2
- B. Configure logging history 3
- C. Configure logging history 4
- D. Configure logging history 5

**Answer: D**

### **Question 11**

Refer to the exhibit.

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

```
service-plane input: CoPP
class-map: PERMIT (match-all)
  50 packets, 3811 bytes
  5 minute offered rate 0000 bps
  Match: access-group 100
class-map: ANY (match-all)
  210 packets, 19104 bytes
  5 minute offered rate 0000 bps, drop rate 0000bps
  Match: access-group 199
  drop
class-map: class-default (match-any)
  348 packets, 48203 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any
```

```
R1#show access-list 100
Extended IP access list 100
 10 permit udp any any eq 23 (100 matches)
 20 permit tcp any any eq telnet (5 matches)
 30 permit tcp any eq telnet any (10 matches)
```

```
R1#show access-list 199
Extended IP access 199
 10 deny tcp any eq telnet any (50 matches)
 50 permit ip any any (1 match)
```

```
R1# show run | section line vty
line vty 0 4
 login
 transport input telnet ssh
 transport output telnet ssh
```

Which two actions restrict access to router R1 by SSH? (Choose two)

- A. Configure **transport input ssh** on line vty and remove sequence 30 from access list 100
- B. Configure **transport output ssh** on line vty and remove sequence 10 from access list 199
- C. Remove **class-map any** from **service-policy CoPP**
- D. Remove sequence 10 from access list 100 and add **sequence 20 deny tcp any any eq telnet** to access list 199
- E. Configure **transport output ssh** on line vty and remove sequence 20 from access list 100

**Answer: A E**

## Question 12

What are two functions of LDP? (Choose two)

- A. It advertises labels per forwarding equivalence class
- B. It is defined in RFC 3038 and 3039
- C. It uses forwarding equivalence class
- D. It must use resource reservation protocol
- E. It requires MPLS traffic engineering

**Answer:** A C

### Question 13

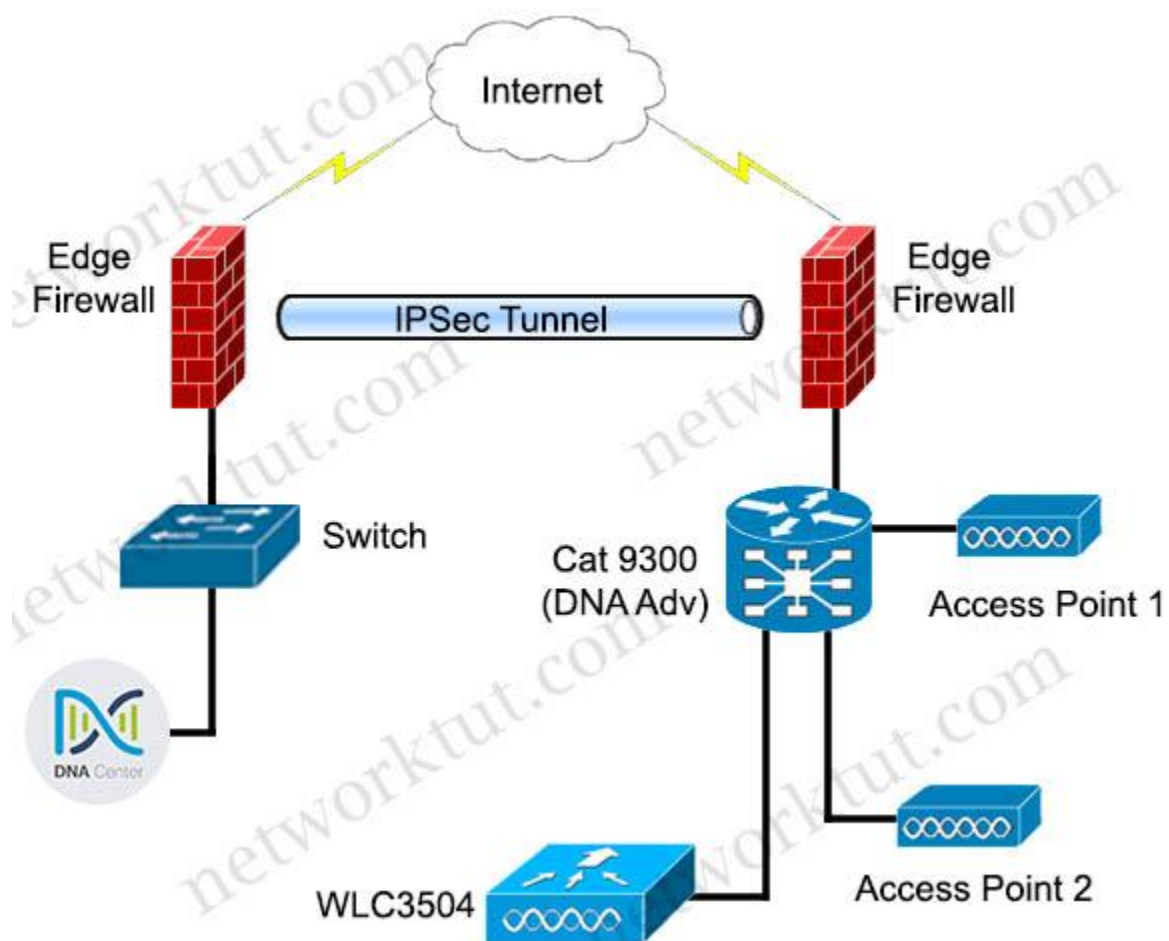
A network administrator is using the DNA Assurance Dashboard panel to troubleshoot an OSPF adjacency that failed between Edge\_NYC interface GigabitEthernet1/3 with Neighbor Edge\_SNJ. The administrator observes that the neighborship is stuck in exstart state. How does the administrator fix this issue?

- A. Configure to match the OSPF interface speed and duplex settings on both routers
- B. Configure to match the OSPF interface unique IP address and subnet mask on both routers.
- C. Configure to match the OSPF interface network types on both routers
- D. Configure to match the OSPF interface MTU settings on both routers

**Answer:** D

### Question 14

Refer to the exhibit.





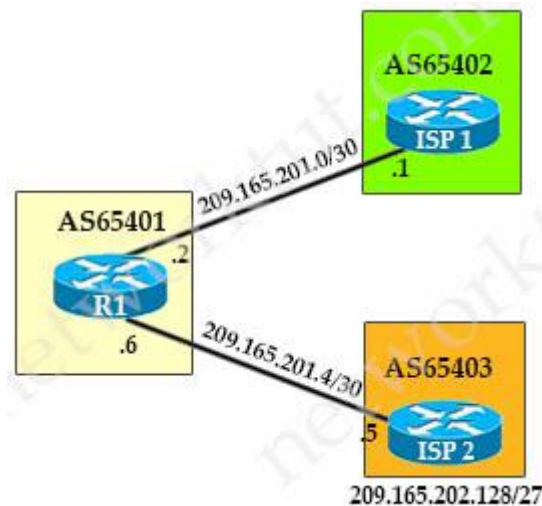
A network is discovering a Cisco catalyst 9300 and a Cisco WLC 3504 in Cisco DNA Center. The 9300 is added successfully but is receiving the error “uncontactable” when the administrator tries to add it in Cisco DNA Center. Which action discovers and resolves the issue?

- A. Copy the .cert file from cisco DNA Center on the USB and upload it to the WLC 3504
- B. Delete the WLC 3504 from cisco DNA center and add it to cisco DNA center again
- C. Add the WLC 3504 under the hierarchy of the catalyst 9300 connected devices
- D. Copy the .pem file from the cisco DNA center on the USB and upload it to the WLC 3504

**Answer: D**

### Question 15

Refer to the exhibit.



```
R1
int G0/0
 ip address 209.165.201.2 255.255.255.252
int G0/1
 ip address 209.165.201.6 255.255.255.252
router bgp 65401
 bgp log-neighbor-changes
 redistribute static
 neighbor 209.165.201.1 remote-as 65402
 neighbor 209.165.201.5 remote-as 65403
 ip route 209.165.200.224 255.255.255.224 Null0
 ip route 209.165.202.128 255.255.255.224 Null0
```

A company with autonomous system number AS65401 has obtained IP address block 209.165.200.224/27 from ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer at ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration on R1 resolves the issue?

A. access-list 10 deny 209.165.202.128 0.0.0.31  
access-list 10 permit any  
!  
router bgp 65401  
neighbor 209.165.201.1 distribute-list 10 out

B. access-list 10 deny 209.165.202.128 0.0.0.31  
access-list 10 permit any  
!  
router bgp 65401  
neighbor 209.165.201.1 distribute-list 10 in

C. ip route 209.165.200.224 255.255.255.224 209.165.201.1  
ip route 209.165.202.128 255.255.255.224 209.165.201.5

D. ip route 0.0.0.0 0.0.0.0 209.165.201.1  
ip route 0.0.0.0 0.0.0.0 209.165.201.5

**Answer: A**

### Question 16

Drag drop the sequence of configuring a policy to avoid following packet forwarding based on the normal routing.

configure set commands	Step 1
configure match commands	Step 2
configure fast switching for PBR	Step 3
configure route map instances	Step 4
configure PBR on the interface	Step 5
configure ACLs	Step 6

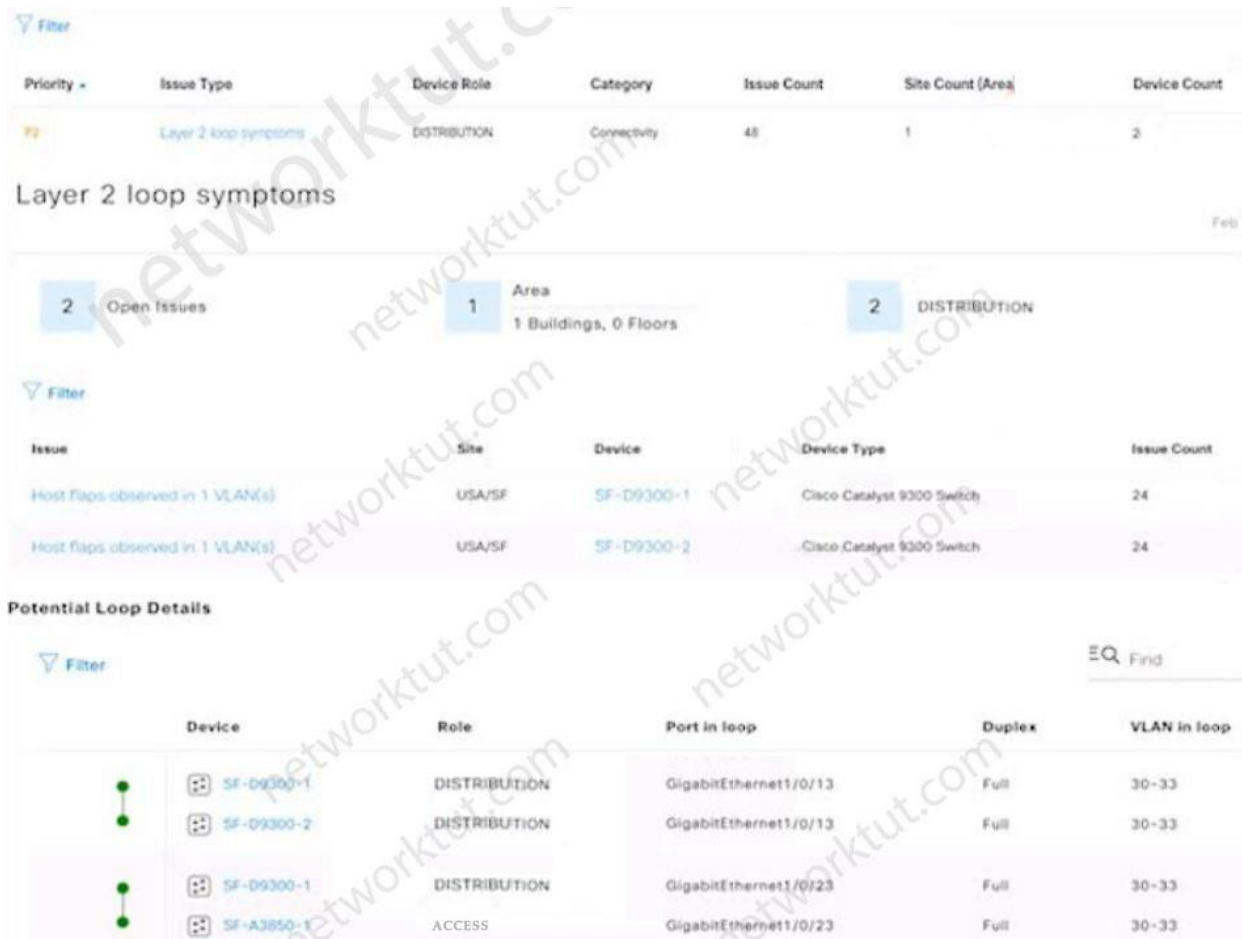
**Answer:**

Step 1 – configure ACLs  
Step 2 – configure route map instances  
Step 3 – configure match commands  
Step 4 – configure set commands

Step 5 – configure PBR on the interface  
Step 6 – configure fast switching for PBR

## Question 17

Refer to the exhibits.



```
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 30-33
 switchport mode trunk
```

```
int GigabitEthernet1/0/23
 switchport trunk allowed vlan 30-33
 switchport mode trunk
```

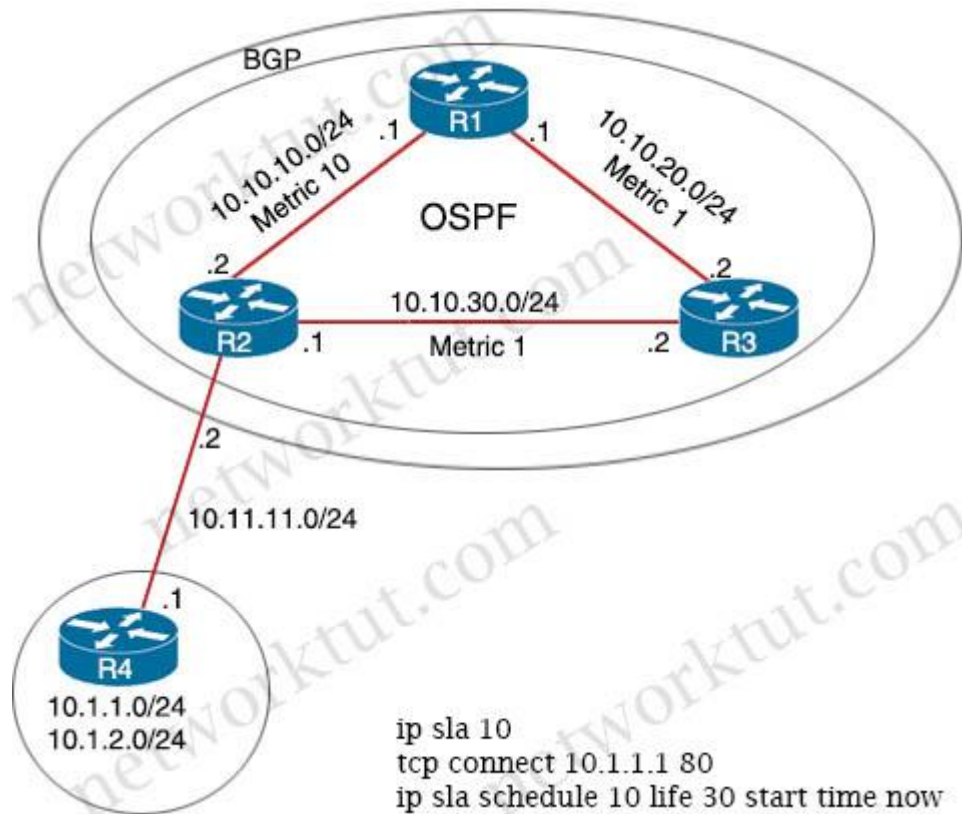
An engineer identified a Layer 2 loop using DNAC. Which command fixes the problem in the SF-D9300-1 Switch?

- A. spanning-tree loopguard default
- B. spanning-tree portfast bpduguard
- C. spanning-tree backbonefast
- D. no spanning-tree uplink fast

**Answer: A**

### Question 18

Refer to the exhibit.



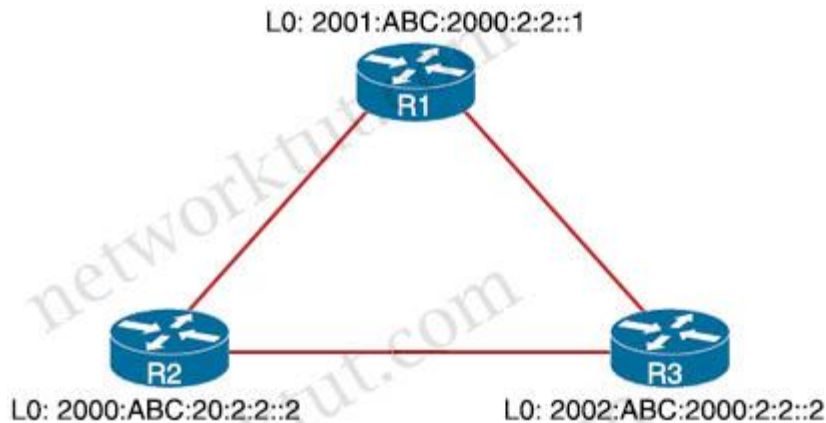
A user has set up an IP SLA probe to test if a non SLA host web server on IP address 10.1.1.1 accepts HTTP sessions prior to deployment. The probe is failing. Which action should the network administrator recommend for the probe to succeed?

- A. Re-issue the ip sla schedule command.
- B. Add icmp-echo command for the host.
- C. Add the control disable option to the tcp connect.
- D. Modify the ip sla schedule frequency to forever.

**Answer: C**

### Question 19

Refer to the exhibit.



#### IPv6 access list PERMIT\_SSH

```

10 deny tcp 2001:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
20 permit tcp 2001:ABC:2000:2:2::/64 host 2000:ABC:20:2:2::2 eq 22
30 deny tcp 2002:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
40 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
50 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
60 permit tcp host 2002:ABC:2000:2:2::2 host 2000:ABC:20:2:2::2 eq 22
70 deny ipv6 any any

```

An IPv6 network was newly deployed in the environment and the help desk reports that R3 cannot SSH to the R2's Loopback interface. Which action resolves the issue?

- A. Modify line 10 of the access list to permit instead of deny.
- B. Remove line 60 from the access list.
- C. Modify line 30 of the access list to permit instead of deny.
- D. Remove line 70 from the access list.

**Answer: C**

#### Question 20

Refer to the exhibit.

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, Ethernet0/0
L   192.168.1.1/32 is directly connected, Ethernet0/0
D   192.168.2.0/24 [90/2297856] via 192.166.12.2.00:02:14, Serial1/1
S   192.168.3.0/24 [1/0] via 192.168.12.2
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.12.0/24 is directly connected, Serial1/1
L   192.168.12.1/32 is directly connected, Serial1/1
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.13.0/24 is directly connected, Serial1/0
L   192.168.13.1/32 is directly connected, Serial1/0
D   192.168.23.0/24 [90/2681856] via 192.168.13.3,00:06:38, Serial1/0
    [90/2681856] via 192.168.12.2, 00:06:38, Serial1/1
D   192.168.24.0/24 [90/2195456] via 192.168.12.2, 00:06:38, Serial1/1

```

All the serial between R1, R2, and R3 D. User on the 192.168.1.0/24 network report slow response times while they access resource on network 192.168.3.0/24. When a traceroute is run on the path. It shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 is still up. What must the network administrator to fix the slowness?

- A. Change the Administrative Distance of EIGRP to 5
- B. Add a static route on R1 using the next hop of R3
- C. Remove the static route on R1
- D. Redistribute the R1 route to EIGRP

**Answer: C**

### Question 21

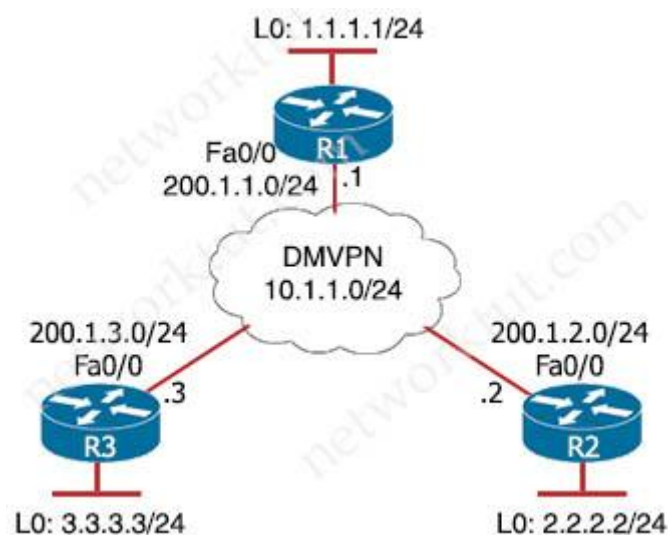
Which feature drops packets if the source address is not found in the snooping table?

- A. Binding Table Recovery
- B. IPv6 Destination Guard
- C. IPv6 Prefix Guard
- D. IPv6 Source Guard

**Answer: D**

### Question 22

Refer to the exhibits.



```

R2:
R2(config)# crypto isakmp policy 10
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# encryption 3des
R2(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R2(cfg-crypto-trans)# mode transport
R2(config)# crypto ipsec profile TST
R2(ipsec-profile)# set transform-set TSET
R2(config)# interface tunnel 123
R2(config-if)# tunnel protection ipsec profile TST

```

When DMVPN is configured, which configuration allows spoke-to-spoke communication using loopback as tunnel source?

- A. Configure crypto isakmp key cisco address 0.0.0.0 on the hub.
- B. Configure crypto isakmp key Cisco address 200.1.0.0 255.255.0.0 on the hub.
- C. Configure crypto isakmp key cisco address 200.1.0.0 255.255.0.0 on the spokes.
- D. Configure crypto isakmp key cisco address 0.0.0.0 on the spokes.

**Answer: D**

### Question 23

Refer to the exhibit.



#### Chicago Router

```

ip route 192.168.1.0 255.255.255.0 10.1.1.2
ip route 192.168.2.0 255.255.255.0 10.1.1.2
!
router eigrp 100
 redistribute static

```

#### LA router

```

ip route 0.0.0.0 0.0.0.0 10.1.1.1

```

A user on the 192.168.1.0/24 network can successfully ping 192.168.3.1, but the administrator cannot ping 192.168.3.1 from the LA router. Which set of configurations fixes the issue?

<b>Option A</b>	<b>Option B</b>
-----------------	-----------------



Chicago Router router eigrp 100 redistribute static metric 10 10 10 10 10	Chicago Router  router eigrp 100 redistribute connected
<b>Option C</b>  Chicago Router  ip route 192.168.3.0 255.255.255.0 10.1.2.2 ip route 192.168.4.0 255.255.255.0 10.1.2.2	<b>Option D</b>  LA Router  ip route 192.168.3.0 255.255.255.0 10.1.1.1 ip route 192.168.4.0 255.255.255.0 10.1.1.1

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

## New ENARSI Questions

### Question 1

Refer to the exhibit. AAA server 10.1.1.1 is configured with the default authentication and accounting settings, but the switch cannot communicate with the server. Which action resolves this issue?

```
Global RADIUS shared secret:*****
retransmission count: 5
timeout value: 10
following RADIUS servers are configured:
  myradius.network.users.com:
    available for authentication on port: 1814
    available for accounting on port: 1813
  10.1.1.1:
    available for authentication on port: 1814
    available for accounting on port: 1813
    RADIUS shared secret: *****
  10.2.2.3
    available for authentication on port: 1814
    available for accounting on port: 1813
  RADIUS shared secret: *****
```



- A. Correct the timeout value
- B. Match the authentication port
- C. Correct the shared secret
- D. Match the accounting port

**Answer: B**

## Question 2

Refer to the exhibit. A company is evaluating multiple network management system tools. Trending graphs generated by SNMP data are returned by the NMS and appear to have multiple gaps. While troubleshooting the issue, an engineer noticed the relevant output. What solves the gaps in the graphs?

```
R1#show policy-map control-plane
Control Plane
Class-map: NMS (match-all)
500461 packets, 24038351 bytes
5 minute offered rate 1390000 bps, drop rate 0 bps
police:
  cir 50000 bps, bc 5000 bytes
  conformed 50444 packets, 24031001 bytes; actions:
    transmit
  exceeded 990012 packets, 94030134 bytes; actions:
    drop
  conformed 4000 bps, exceed 0 bps
```

- A. Remove the class map NMS from being part of control plane policing
- B. Remove the exceed-rate command in the class map
- C. Configure the CIR rate to a lower value that accommodates all the NMS tools
- D. Separate the NMS class map in multiple class maps based on the specific protocols with appropriate CoPP actions

**Answer: D**

## Question 3

Drag and drop the credentials from the left onto the remote login information on the right to resolve a failed login attempt to vtys. Not all credentials are used.

```
aaa new-model
aaa authentication login default none
aaa authentication login telnet local
!
username cisco password 0 Ocsic
!
line vty 0
```

```

password LetMeIn
login authentication telnet
transport input telnet
line vty 1
password LetMeIn
transport input telnet

```

no password	vty 0
0csic	username
no username	password
LetMeIn	vty 1
cisco	username
LetMeIn	password

**Answer:**

**vty 0:**

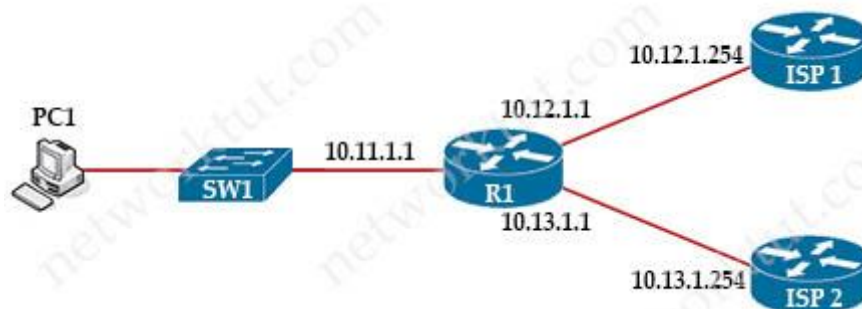
+ cisco  
+ 0csic

**vty 1:**

+ no username  
+ no password

#### Question 4

Refer to the exhibit. An engineer is monitoring reachability of the configured default routes to ISP1 and ISP2. The default route from ISP1 is preferred if available. How is this issue resolved?



```

R1
ip sla 100

```

```

icmp-echo 10.12.1.254
!
track 10 ip sla 100 reachability
!
ip route 0.0.0.0 0.0.0.0 10.12.1.254 track 10
ip route 0.0.0.0 0.0.0.0 10.13.1.254 10
!
R1#show ip route
--Output Omitted--
Gateway of last resort is 10.13.1.254 to network 0.0.0.0

S* 0.0.0.0/0 [10/0] via 10.13.1.254
    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.11.1.0/24 is directly connected, GigabitEthernet0/1
L    10.11.1.1/32 is directly connected, GigabitEthernet0/1
C    10.12.1.0/24 is directly connected, GigabitEthernet0/0
L    10.12.1.1/32 is directly connected, GigabitEthernet0/0
C    10.13.1.0/24 is directly connected, GigabitEthernet0/2
L    10.13.1.1/32 is directly connected, GigabitEthernet0/2

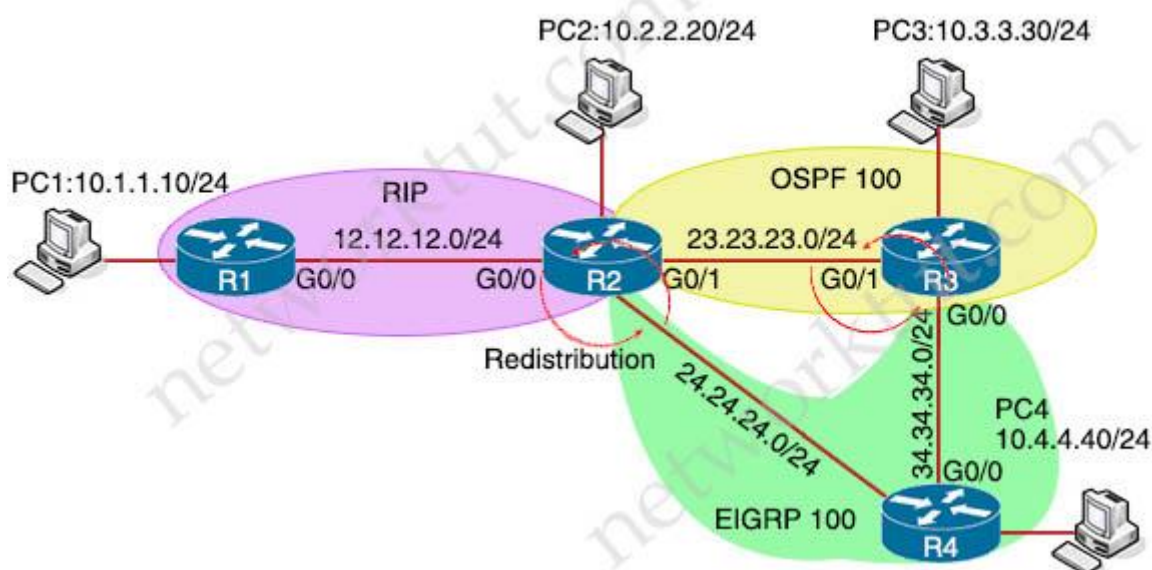
```

- A. Use the icmp-echo command to track both default routes
- B. Start IP SLA by matching numbers for track and ip sla commands
- C. Start IP SLA by defining frequency and scheduling it
- D. Use the same AD for both default routes

**Answer: C**

### Question 5

Refer to the exhibit. Redistribution is enabled between the routing protocols, and now PC2 PC3, and PC4 cannot reach PC1. What are the two solutions to fix the problem? (Choose two)



- A. Filter RIP and OSPF routes back into OSPF from EIGRP when redistributing into OSPF in R2

- B. Filter all routes except EIGRP routes when redistributing into OSPF in R3
- C. Filter OSPF routes into RIP from EIGRP when redistributing into RIP in R2
- D. Filter all routes except RIP routes when redistributing into EIGRP in R2
- E. Filter RIP routes back into RIP when redistributing into RIP in R2

**Answer:** C E

### Question 6

Which label operations are performed by a label edge router?

- A. PUSH and PHP
- B. SWAP and POP
- C. SWAP and PUSH
- D. PUSH and POP

**Answer:** D

### Question 7

Refer to the exhibit. The network administrator configured VRF lite for customer A. The technician at the remote site misconfigured VRF on the router. Which configuration will resolve connectivity for both sites of customer A?

```
ip vrf customer_a
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
interface FastEthernet0.1
  encapsulation dot1Q 2
  ip vrf forwarding customer_a
  ip address 192.168.4.1 255.255.255.0
!
router ospf 1
  log-adj adjacency-changes
!
  router ospf 2 vrf customer_a
  log-adj adjacency-changes
  network 192.168.4.0 0.0.0.255 area 0
!
end
```

- A.
- ip vrf customer\_a
- rd 1:2
- route-target both 1:1

B.

```
ip vrf customer_a
rd 1:2
route-target both 1:2
```

C.

```
ip vrf customer_a
rd 1:1
router-target import 1:1
router-target export 1:2
```

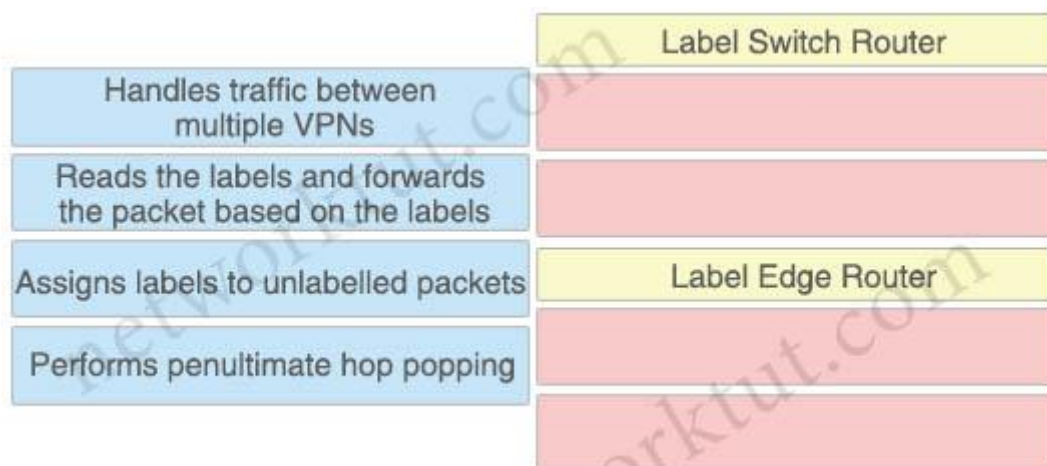
D.

```
ip vrf customer_a
rd 1:1
route-target export 1:2
router-target import 1:2
```

**Answer: A**

### Question 8

Drag and drop the operations from the left onto the locations where the operations are performed on the right.



**Answer:**

#### Label Switch Router:

- + Reads the labels and forwards the packet based on the labels
- + Performs penultimate hop popping

**Label Edge Router:**

- + Handles traffic between multiple VPNs
- + Assigns labels to unlabelled packets

**Question 9**

After some changes in the routing policy, it is noticed that the router in AS 45123 is being used as a transit AS router for several service providers. Which configuration ensures that the branch router in AS 45123 advertises only the local networks to all SP neighbors?

A.

```
ip as-path access-list 1 permit ^45123$  
!  
router bgp 45123  
neighbor SP-Neighbors filter-list 1 out
```

B.

```
ip as-path access-list 1 permit ^45123  
!  
router bgp 45123  
neighbor SP-Neighbors filter-list 1 out
```

C.

```
ip as-path access-list 1 permit ^$  
!  
router bgp 45123  
neighbor SP-Neighbors filter-list 1 out
```

D.

```
ip as-path access-list 1 permit  
!  
router bgp 45123  
neighbor SP-Neighbors filter-list 1 out
```

**Answer: C**

**Question 10**

Refer to the exhibit. An engineer is trying to get a packet destined for 192.168.32.100 forwarded through 10.1.1.1, but it was forwarded through 10.1.1.2. What action forwards the packets through 10.1.1.1?

```
Router#show ip route  
...  
D 192.168.32.0/19 [90/25789217] via 10.1.1.1  
R 192.168.32.0/24 [120/4] via 10.1.1.2
```

O 192.168.32.0/26 [110/229840] via 10.1.1.3

- A. Configure EIGRP to receive 192.168.32.0 route with lower metric
- B. Configure EIGRP to receive 192.168.32.0 route with lower administrative distance
- C. Configure EIGRP to receive 192.168.32.0 route with equal or longer prefix than /24
- D. Configure EIGRP to receive 192.168.32.0 route with longer prefix than /19

**Answer: C**

### Question 11

Refer to the exhibit. A junior engineer updated a branch router configuration. Immediately after the change, the engineer receives calls from the help desk that branch personnel cannot reach any network destinations. Which configuration restores service and continues to block 10.1.1.100/32?

```
BRANCH-RTR#
router eigrp 100
 network 10.4.31.0 0.0.0.7
 network 10.100.100.1 0.0.0.0
 distribute-list route-map FILTER-IN in FastEthernet0/0
 eigrp router-id 10.100.100.1
!
ip prefix-list 102 seq 10 permit 10.1.1.100/32
!
route-map FILTER-IN deny 10
 match ip address prefix-list 102
```

- A. ip prefix-list 102 seq 15 permit 0.0.0.0/32 le 32
- B. route-map FILTER-IN permit 20
- C. ip prefix-list 102 seq 5 permit 0.0.0.0/32 le 32
- D. route-map FILTER-IN deny 5

**Answer: B**

### Question 12

An engineer configured a leak-map command to summarize EIGRP routes and advertise specifically loopback 0 with an IP of 10.1.1.1 255.255.255.252 along with the summary route. After finishing configuration, the customer complained not receiving summary route with specific loopback address. Which two configurations will fix it? (Choose two)

```
router eigrp 1
```

```
!  
route_map Leak-Route deny 10  
!  
interface Serial 0/0  
ip summary-address eigrp 1 10.0.0.0 255.0.0.0 leak-map Leak-Route
```

- A. Configure route-map Leak-Route permit 10 and match access-list 1
- B. Configure access-list 1 permit 10.1.1.1 0.0.0.252
- C. Configure access-list 1 and match under route-map Leak-Route
- D. Configure route-map Leak-Route permit 20
- E. Configure access-list 1 permit 10.1.1.0 0.0.0.3

**Answer:** A E

### Question 13

Refer to the exhibit. An IP SLA is configured to use the backup default route when the primary is down, but it is not working as desired. Which command fixes the issue?

```
R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1  
R1(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.2 10  
R1(config)#ip sla 1  
R1(config)#icmp-echo 1.1.1.1 source-interface FastEthernet0/0  
R1(config)#ip sla schedule 1 life forever start-time now  
R1(config)#track 1 ip sla 1 reachability
```

- A. R1(config)# ip route 0.0.0.0 0.0.0.0 1.1.1.1 track 1
- B. R1 (config)# ip route 0.0.0 0 0.0.0 0 2.2.2 2
- C. R1 (config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2 10 track 1
- D. R1(config)# ip sla track 1

**Answer:** A

### Question 14

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 3 and updates routing protocols
- C. It has sub-second failure detection for layer 1 and layer 2 problems
- D. It has sub-second failure detection for layer 1 and layer 3 problems



**Answer: B**

### Question 15

Refer to the exhibit. The ACL is placed on the inbound GigabitEthernet 0/1 interface of the router. Host 192.168.10.10 cannot SSH to host 192.168.100.1 even though the flow is permitted. Which action resolves the issue without opening full access to this router?

```
ip access-list extended FILTER
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 22
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 23
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 80
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 443
permit tcp host 192.168.10.10 host 192.168.100.10 eq ssh
permit ip any any
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip access-group FILTER in
```

- A. Temporarily move the permit ip any any line to the beginning of the ACL to see if it the flow works
- B. Run the show access-list FILTER command to view if the SSH entry has any hit statistics associated with it
- C. Move the SSH entry to the beginning of the ACL
- D. Temporarily remove the ACL from the interface to see if the flow works

**Answer: C**

### Question 16

Which component of MPLS VPN is used to extend the IP address so that an engineer is able to identify to which VPN it belongs?

- A. RD
- B. VPNv4 address family
- C. RT
- D. LDP

**Answer: A**

### Question 17

Refer to the exhibit. BGP is flapping after the CoPP policy is applied. What are the two solutions to fix the issue? (Choose two)

```
policy-map COPP-7600
  class COPP-CRITICAL-7600
    police cir 2000000 bc 62500
    conform-action transmit
    exceed-action transmit
  !
class class-default
  police cir 2000000 bc 6250
  conform-action transmit
  exceed-action drop
!
class-map match-all COPP-CRITICAL-7600
  match access-group name COPP-CRITICAL-7600
!
ip access-list extended COPP-CRITICAL-7600
  permit ip any any eq http
  permit ip any any eq https
```

- A. Configure BGP in the COPP-CRITICAL-7600 ACL
- B. Configure a higher value for CIR under the default class to allow more packets during peak traffic
- C. Configure a higher value for CIR under the class COPP-CRITICAL-7600
- D. Configure a three-color policer instead of two-color policer under class COPP-CRITICAL-7600
- E. Configure IP CEF to CoPP policy and BGP to work

**Answer:** A B

### Question 18

During the maintenance window, an administrator accidentally deleted the telnet-related configuration that permits a Telnet connection from the inside network (Eth 0/0) to the outside of the network between Friday-Sunday night hours only. Which configuration resolves the issue?

- A.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
changewindow
!
time-range changewindow
periodic 22:00 to 05:00
```
- B.

```
interface Ethernet0/0
```

```
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
changewindow
!
time-range changewindow
periodic Friday Saturday Sunday 22:00 to 05:00
```

C.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
changewindow
!
time-range changewindow
periodic Friday Saturday Sunday 22:00 to 05:00
```

D.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
changewindow
!
time-range changewindow
periodic Friday Saturday Sunday
```

**Answer: B**

### **Question 19**

Refer to the exhibit. Which action resolve intermittent connectivity observed with the SNMP trap packets?

```
R3#show policy-map control-plane
```

```
Service-policy output: R3_CoPP
```

```
Class-map: mgmt (match-all)
```

```
361 packets, 73858 bytes
```

```
5 minute offered rate 0 bps, drop rate 0bps
```

```
Match: access-group 20
```

```
police:
```

```
  cir 8000 bps, bc 1500 bytes, be 1500 bytes
```

```
  conformed 8 packets, 1506 bytes; actions:
```

```
    transmit
```

```
  exceeded 353 packets, 72352 bytes; actions:
```

```
    drop
```

```
  violated 0 packets, 0 bytes; actions:
```

```
    drop
```

```
  conformed 0 bps, exceed 0 bps, violate 0 bps
```

```
Class-map: class-default (match-any)
```

```
124 packets, 10635 bytes
```

```
5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: any
```

```
R3#show access-lists 120
```

```
Extended IP access list 120
```

```
10 permit udp any any eq snmptrap (361 matches)
```

- A. Add a new class map to match TCP traffic
- B. Add one new entry in the ACL 120 to permit the UDP port 161
- C. Increase the CIR of the mgmt class map
- D. Decrease the committed burst size of the mgmt class map

**Answer: C**

### Question 20

An engineer configured a company's multiple area OSPF head office router and Site A cisco routers with VRF lite. Each site router is connected to a PE router of an MPLS backbone. After finishing both site router configurations, none of the LSA 3,4 5, and 7 are installed at Site A router.

```

Head Office and Site A:
ip cef
ip vrf abc
rd 101:101
!
interface FastEthernet0/0
ip vrf forwarding abc
ip address 172.16.16.x 255.255.255.252
!
router ospf 1 vrf abc
log-adjacency-changes
network 172.16.16.0 0.0.0.255 area 1

```

Which configuration resolves this issue?

- A. configure **capability vrf-lite** on Site A and its connected PE router under **router ospf 1 vrf abc**
- B. configure **capability vrf-lite** on Head Office and its connected PE router under **router ospf 1 vrf abc**
- C. configure **capability vrf-lite** on both PE routers connected to Head Office and Site A routers under **router ospf 1 vrf abc**
- D. configure **capability vrf-lite** on Head Office and Site A routers under **router ospf 1 vrf abc**

**Answer: D**

## Question 21

Drag and drop the MPLS VPN device types from me left onto the definitions on the right.

CE device	device in the enterprise network that connects to other customer devices
Customer (C) device	device in the core of the provider network that switches MPLS packets
Provider (P) device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device at the edge of the enterprise network that connects to the SP network

**Answer:**

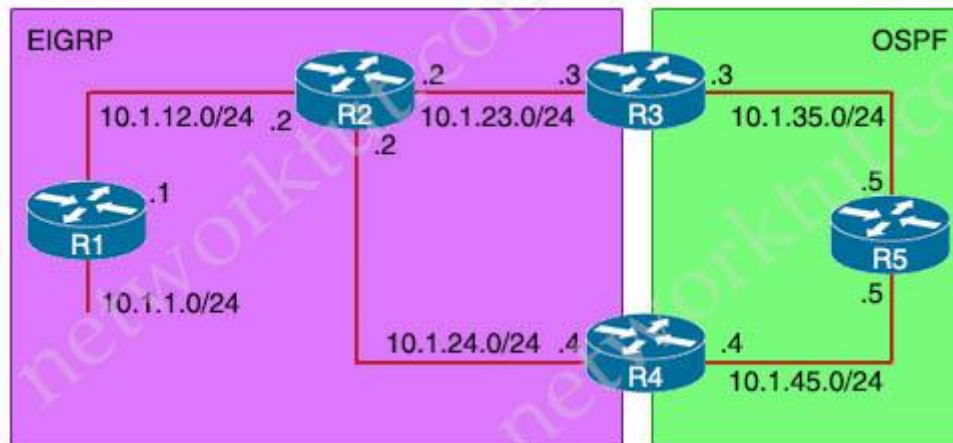
- + device in the enterprise network that connects to other customer devices: Customer (C) device
- + device in the core of the provider network that switches MPLS packets: Provider (P) device
- + device that attaches and detaches the VPN labels to the packets in the provider network: PE

device

+ device at the edge of the enterprise network that connects to the SP network: CE device

### Question 22

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?



```
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 10.1.35.0 0.0.0.0 area 0
```

- A. Change the administrative distance of OSPF to 200 on R5
- B. Change the administrative distance of the external EIGRP to 90
- C. Apply the outbound distribution list on R5 toward R4 in OSPF
- D. Redistribute OSPF into EIGRP on R4

Answer: B

### Question 23

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**

### Question 24

Refer to the exhibit.

```
Device# 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	01:33:23	S
1	172.18.46.2	192.168.1.4	UP	00:23:03	D

An engineer has configured DMVPN on a spoke router. What is the WAN IP address of another spoke router within the DMVPN network?

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

**Answer: D**

### Question 25

Refer to the exhibit.

```
*Jul 23 09:33:34.530: IF-EvD(GigabitEthernet0/0): reports state transition from DOWN to DOWN
*Jul 23 09:33:35.525: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jul 23 09:33:35.528: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jul 23 09:33:36.215: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jul 23 09:33:37.996: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
```

```
*Jul 23 09:33:38.006: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to UP
*Jul 23 09:33:38.998: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1. What action will fix the issue?

- 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**

### Question 26

Refer to the exhibit.

```
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
!
```

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

- A. Configure the server with a static IP address and default gateway
- B. Configure the server to use DHCP on the network with default gateway 200.30.40.100
- 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: A C**

### Question 27



Which protocol does MPLS use to support traffic engineering?

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

**Answer: D**

### Question 28

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:**

- + 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 ND Inspection
- + Filter inbound traffic on Layer 2 switch port that are not in the IPv6 binding table: IPv6 Source Guard
- + 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: IPv6 Binding Table

### Question 29

Refer to the exhibit.

**R3#show policy-map control-plane**

Control Plane

Service-policy output: R3\_CoPP

Class-map: SNMP-Out (match-all)

124 packets, 3345 bytes

5 minute offered rate 0 bps, drop rate 0bps

Match: access-group name SNMP

police:

cir 8000 bps, bc 1500 bytes, be 1500 bytes

conformed 0 packets, 0 bytes; actions:

transmit

exceeded 0 packets, 0 bytes; actions:

drop

conformed 0 bps, exceed 0 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 access-lists SNMP**

Extended IP access list SNMP

10 permit udp any eq snmp any

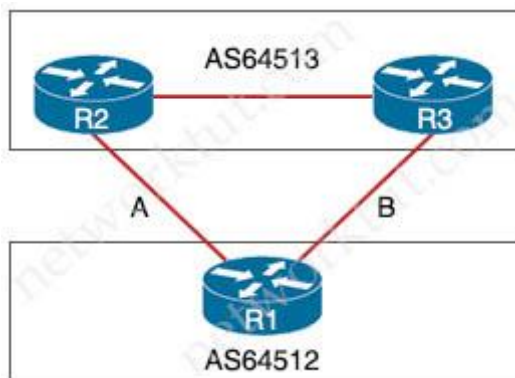
R1 is being monitored using SNMP and monitoring devices are getting only partial information. What action should be taken to resolve this issue?

- A. Modify the access list to include snmptrap
- B. Modify the CoPP policy to increase the configured exceeded limit for SNMP
- 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: A**

### **Question 30**

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. Traffic should flow via the backup link toward the ASN. Which BGP configuration on R1 accomplishes this goal?

<b>Option A</b> <pre>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</pre>	<b>Option B</b> <pre>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</pre>
<b>Option C</b> <pre>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</pre>	<b>Option D</b> <pre>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</pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

### Question 31

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

```

MASS-RTR#show running-oonfig
!
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 0236244828115F3348
username cisco privilege 15 password 7 0607072C394A5B
archive
 log oonfig
 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: A**

### Question 32

Which IGPs are supported by the MPLS LDP autoconfiguration feature?

- A. ISIS and RIPv2
- B. RIPv2 and OSPF
- C. OSPF and ISIS
- D. OSPF and EIGRP

**Answer: C**

### **Question 33**

What does the PE router convert the IPv4 prefix to within an MPLS VPN?

- A. 48-bit route combining the IP and PE router-id
- B. VPN-IPv4 prefix combined with the 64-bit route distinguisher
- C. eBGP path association between the PE and CE sessions
- D. prefix that combines the ASN, PE router-id, and IP prefix

**Answer: B**

### **Question 34**

Refer to the exhibit.

```
Router#show access-lists
Standard IP access list 1
  10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, deny, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#
```

Which two actions should be taken to access the server? (Choose two)

- A. Modify the access list to add a second line of permit ip any any
- B. Modify the access list to deny the route to 192.168.2.2
- C. Modify distribute list seq 10 to permit the route to 192.168.2.2
- D. Add a sequence 20 in the route map to permit access list 1
- E. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF

**Answer:** B E (maybe this question is missing some information)

### Question 35

Refer to the exhibit.

```
R1
ip prefix-list ccnp1 seq 5 permit 10.1.48.0/24 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.0/24 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.0/24 le 24

route-map ospf-to-eigrp permit 10
 match ip address prefix-list ccnp1
 set tag 30
route-map ospf-to-eigrp permit 20
 match ip address prefix-list ccnp2
 set tag 20
route-map ospf-to-eigrp permit 30
 match ip address prefix-list ccnp3
 set tag 10
```

An engineer wanted to set a tag of 30 to route 10.1.80.65/32 but it failed. How is the issue fixed?

- A. Modify route-map ospf-to-eigrp permit 30 and match prefix-list ccnp2.
- B. Modify route-map ospf-to-eigrp permit 10 and match prefix-list ccnp2.
- C. Modify prefix-list ccnp3 to add 10.1.64.0/20 le 24
- D. Modify prefix-list ccnp3 to add 10.1.64.0/20 ge 32

**Answer:** B

### Question 36

What does IPv6 Source Guard utilize to determine if IPv6 source addresses should be forwarded?

- A. Binding Table
- B. ACLS
- C. ACE
- D. DHCP

**Answer:** A

### Question 37

An engineer needs dynamic routing between two routers and is unable to establish OSPF adjacency. The output of the **show ip ospf neighbor** command shows that the neighbor state is EXSTART/EXCHANGE. Which action should be taken to resolve this issue?

- A. match the passwords
- B. match the hello timers
- C. match the MTUs
- D. match the network types

**Answer: C**

### Question 38

Refer to the exhibit.

<b>Option A</b> <pre> ipv6 access-list inbound permit tcp any any established deny ipv6 any any log ! interface gi0/0 ipv6 traffic-filter inbound out </pre>	<b>Option B</b> <pre> ipv6 access-list inbound permit tcp any any syn deny ipv6 any any log ! interface gi0/0 ipv6 traffic-filter inbound out </pre>
<b>Option C</b> <pre> ipv6 access-list inbound permit tcp any any established deny ipv6 any any log ! interface gi0/0 ipv6 traffic-filter inbound in </pre>	<b>Option D</b> <pre> ipv6 access-list inbound permit tcp any any syn deny ipv6 any any log ! interface gi0/0 ipv6 traffic-filter inbound in </pre>

A network administrator configured an IPv6 access list to allow TCP return frame only, but it is not working as expected. Which changes resolve this issue?

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

### Question 39

Refer to the exhibit.

```
Router#show running-config
Building configuration...
!
<output omitted>
!
hostname R1
!
ip domain-name networktut.com
!
crypto key generate rsa modulus 2048
!
username admin privilege 15 secret cisco123
!
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 1 deny any log
!
line vty 0 15
access-list 1 in
login local
!
<output omitted>
!
end
```

A user cannot SSH to the router. What action must be taken to resolve this issue?

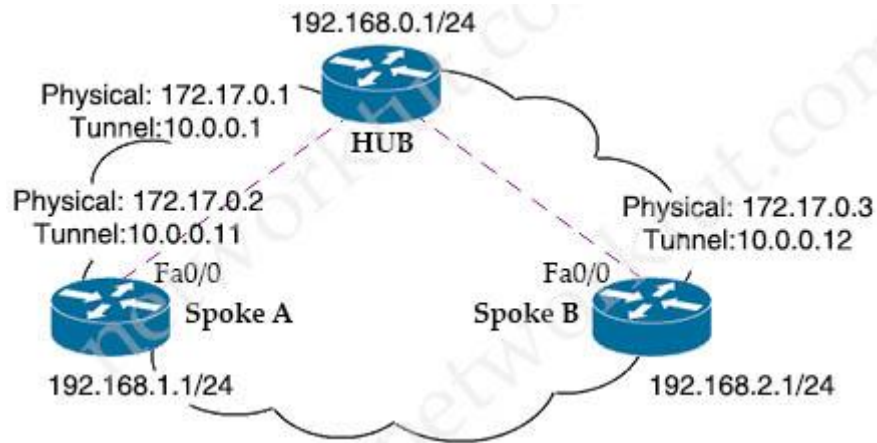
- A. Configure transport input ssh
- B. Configure transport output ssh
- C. Configure ip ssh version 2
- D. Configure ip ssh source-interface loopback0

**Answer:** A

#### **Question 40**

Refer to the exhibit. Which interface configuration must be configured on the HUB router to enable DMVPN with mGRE mode?





<p><b>Option A</b></p> <pre> interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.1.0.1 255.255.255.0 ip nhrp map multicast dynamic ip nhrp network-id 1 tunnel source 172.17.0.1 ip nhrp map 10.0.0.11 172.17.0.2 ip nhrp map 10.0.0.12 172.17.0.3 tunnel mode gre </pre>	<p><b>Option B</b></p> <pre> interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.0.0.1 255.255.255.0 ip nhrp map multicast dynamic ip nhrp network-id 1 tunnel source 10.0.0.1 tunnel mode gre multipoint </pre>
<p><b>Option C</b></p> <pre> interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.0.0.1 255.255.255.0 ip nhrp network-id 1 tunnel source 172.17.0.1 tunnel mode gre multipoint </pre>	<p><b>Option D</b></p> <pre> interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.0.0.1 255.255.255.0 ip nhrp map multicast dynamic ip nhrp network-id 1 tunnel source 10.0.0.1 tunnel destination 172.17.0.2 tunnel mode gre multipoint </pre>

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

#### Question 41

Refer to the exhibit.

```
interface Ethernet0/0
```

```

ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
time-range Office-hour
  periodic weekdays 08:00 to 17:00
!
access-list 101 permit tcp 10.0.0.0 0.0.0.0 172.16.1.0 0.0.0.255 eq ssh time-
range Office-hour

```

An IT staff member comes into the office during normal office hours and cannot access devices through SSH. Which action should be taken to resolve this issue?

- A. Modify the access list to use the correct IP address
- B. Configure the correct time range
- C. Modify the access list to correct the subnet mask
- D. Configure the access list in the outbound direction

**Answer: A**

#### Question 42

Refer to the exhibit.

```

R1#show run | begin line
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
transport preferred telnet
transport output none
stopbits 0 4
!
line vty 0 4
login
transport preferred telnet
transport input none
transport output telnet
R1#

R1#ssh -l cisco 192.168.12.2
%ssh connections not permitted from this terminal
R1#

```

#### Option A

```

R1(config)#line console 0
R1(config-line)#transport preferred ssh

```

#### Option B

```

R1(config)#line vty 0
R1(config-line)#transport output ssh

```

#### Option C

#### Option D

R1(config)#line vty 0 R1(config-line)#transport output ssh R1(config-line)#transport preferred ssh	R1(config)#line console 0 R1(config-line)#transport output ssh
--	---

An engineer receives this error message when trying to access another router m-band from the serial interface connected to the console of R1. Which configuration is needed on R1 to resolve this issue?

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

## OSPF & EIGRP Questions

<https://www.networktut.com/ospf-eigrp-questions>

### Question 1

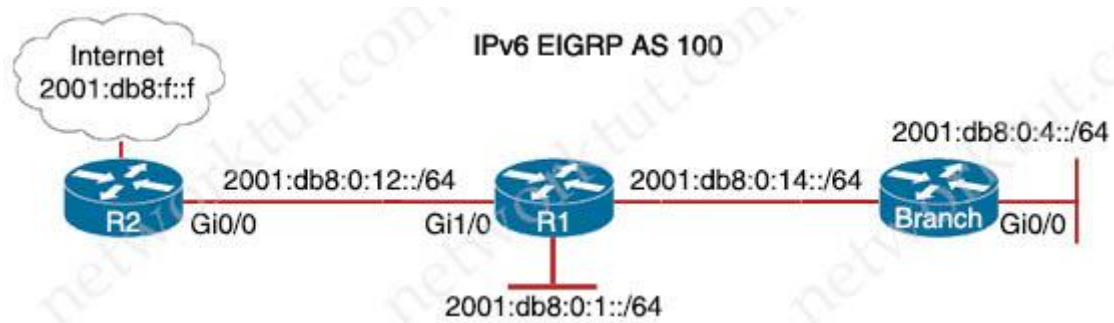
Which configuration adds an IPv4 interface to an OSPFv3 process in OSPFv3 address family configuration?

- A.  
router ospfv3 1  
address-family ipv4
- B. Router(config-router)#ospfv3 1 ipv4 area 0
- C. Router(config-if)#ospfv3 1 ipv4 area 0
- D.  
router ospfv3 1  
address-family ipv4 unicast

**Answer: C**

### Question 2

Refer to the exhibit. User in the branch network of 2001:db8:0:4 report 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 – Rely,

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, GigabitEthernet0/0

#### 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 – Rely,

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**

#### Question 3

Refer to the exhibit. An engineer configuration a static route on a router, but when the engineer checks the route to the destination, a different next hop is chosen. What is the reason for this?

```
Router#show running-config | include ip route
ip route 192.168.2.2 255.255.255.255 209.165.200.225 130
Router#show ip route
```

---output omitted---

Gateway of last resort is not set

```
192.168.1.0/32 is subnetted, 1 subnets
C    192.168.1.1 is directly connected, Loopback0
192.168.2.0/32 is subnetted, 1 subnets
O    192.168.2.2 [110/11] via 192.168.12.2,00:33:32, Ethernet0/0
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/24 is directly connected, Ethernet0/0
L    192.168.12.1/32 is directly connected, Ethernet0/0
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.0/24 is directly connected, Ethernet0/1
    209.165.200.226/32 is directly connected, Ethernet0/1
```

- A. The configured AD for the static route is higher than the AD of OSPF
- B. The metric of the OSPF route is lower than the metric of the static route
- C. Dynamic routing protocol always have priority over static routes
- D. The syntax of the static route is not valid do the route is not considered

**Answer: A**

#### Question 4

Refer to the exhibit. An engineer is trying to generate a summary route in OSPF for network 10.0.0.0/8, but the summary route does not show up in the routing table. Why is the summary route missing?

Router#**show ip route**

Gateway of last resort is not set

```
192.168.1.0/32 is subnetted, 1 subnets
O    192.168.1.1[110/11] via 192.168.12.1,13:32:22, Ethernet0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, Loopback0
L    192.168.2.2/32 is directly connected, Loopback0
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, Ethernet0/1
L    192.168.3.1/32 is directly connected, Ethernet0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/24 is directly connected, Ethernet0/0
L    192.168.12.2/32 is directly connected, Ethernet0/0
```

Router#**show running-config | section ospf**

```
router ospf 1
summary-address 10.0.0.0 255.0.0.0
redistribute static subnets
network 192.168.3.0 0.0.0. 255 area 0
network 192.168.12.0 0.0.0. 255 area 0
Router#
```

- A. The summary route is not visible on this router, but it is visible on other OSPF routers in the same area
- B. The summary-address command is used only for summary prefixes between areas
- C. The summary route is visible only in the OSPF database not in the routing table
- D. There is no route for a subnet inside 10.0.0.0/8, so the summary route is not generated

**Answer: D**

### Question 5

Refer to the exhibit. 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

**Answer: B**

## BGP Questions

<https://www.networktut.com/bgp-questions>

### Question 1

Refer to the exhibit. R2 is a route reflector, and R1 and R3 are route reflector clients. The router R2 learns the route to 172.16.25.0/24 from R1, but it does not advertise to R3. What is the reason the route is not advertised?

R2#**show ip bgp**

BGP table version is 4, local router ID is 209.65.200.225

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,

r RIB-failure, S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

	Network	Next Hop	Metric	LocPrf	Weight	Path
* i	172.16.25.0/24	209.165.200.225	0	100	0	?

R3#**show ip bgp summary**

BGP router identifier 192.168.3.3, local AS number 65000

BGP table version is 4, main routing table version 4

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
State/PfxRcd								

192.168.2.2      4 65000      8      7      4      0      0 01:00:18      0

- A. Route reflector setup requires full BGP mesh between the routers
- B. In route reflector setup only classification prefix are advertised from one client to another
- C. In route reflector setup only classful prefix are advertised to other clients
- D. R2 does not have a route to the next hop, so R2 does not advertise the prefix to the clients

**Answer: D**

## Question 2

Refer to the exhibit. Which control plan policy limits BGP traffic that is destined to the CPU to 1 Mbps and ignores BGP traffic that is higher rate?

Cat3850-Stack-2#**show policy-map**

```
Policy Map LIMIT_BGP
Class BGP
drop
```

```
Policy Map SHAPE_BGP
Class BGP
Average Rate Traffic Shaping
cir 10000000 (bps)
```

```
Policy Map POLICE_BGP
Class BGP
police cir 1000k bc 1500
conform-action transmit
exceed-action transmit
```

```
Policy Map COPP
Class BGP
police cir 1000k bc 1500
conform-action transmit
exceed-action drop
```

- A. policy-map SHAPE\_BGP
- B. policy-map LIMIT\_BGP
- C. policy-map POLICE\_BGP
- D. policy-map COPP

**Answer: D**

## Question 3

Refer to the exhibit. A router receiving BGP routing updates from multiple neighbors for routers in AS 690. What is the reason that the router still sends traffic that is destined to AS 690 to a neighbor other than 10.222.10.1?

!

```

neighbor 10.222.1.1 route-map SET-WEIGHT in
neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800$
!
route-map SET-WEIGHT permit 10
  match as-path 200
  set local-preference 250
  set weight 200

```

- A. The local preference value in another neighbor statement is higher than 250
- B. The local preference value should be set to the same value as the weight in the route map
- C. The route map is applied in the wrong direction
- D. The weight value in another statement is higher than 200

**Answer: D**

#### Question 4

Refer to the exhibit. What is the result if applying this configuration?

R1#**show policy-map control-plane**

Control Plane

Service-policy input: CoPP-BGP

```

Class-map: BGP (match-all)
  2716 packets, 193843 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name BGP
drop

```

```

Class-map: class-default (match-any)
  5212 packets, 64484847 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

```

- A. The router can form BGP neighborships with any other device.
- B. The router can form BGP neighborships with any device that matched by the access list named "BGP"
- C. The router cannot form BGP neighborships with any other device
- D. The router cannot form BGP neighborships with any device that is matched by the access list named "BGP"

**Answer: D**

#### Question 5

Refer to the exhibit, in which circumstance does the BGP neighbor remain in the idle condition?



```
R200#show ip bgp summary
```

```
BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 26, main routing table version 26
1 network entries using 132 bytes of memory
1 path entries using 52 bytes of memory
2/1 BGP path/bestpath attribute entries using 296 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 28 bytes of memory
BGP using 508 total bytes of memory
BGP activity 24/23 prefixes, 24/23 paths, scan interval 60 secs
Neighbor  V AS      MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.0.2.2  4 65100  20335   20329    0      0     0    00:02:04 Idle(PfxCt)
```

```
R200#
```

- A. if prefixes are not received from the BGP peer
- B. if prefixes reach the maximum limit
- C. if a prefix list is applied on the inbound direction
- D. if prefixes exceed the maximum limit

**Answer: D**

## Route-map Questions

<https://www.networktut.com/route-map-questions>

### Question 1

R2 has a locally originated prefix 192.168.130.0/24 and has these configurations:

```
ip prefix-list test seq 5 permit 192.168.130.0/24
route-map OUT permit 10
match ip address prefix-list test
set as-path prepend 65000
```

What is the result when the route-map OUT command is applied toward an eBGP neighbor R1 (1.1.1.1) by using the “neighbor 1.1.1.1 route-map OUT out” command?

- A. R1 sees 192.168.130.0/24 as two hops away instead of one AS hop away
- B. R1 does not forward traffic that is destined for 192.168.130.0/24
- C. Network 192.168.130.0/24 is not allowed in the R1 table
- D. R1 does not accept any route other than 192.168.130.0/24

**Answer: A**

### Question 2

Refer to the exhibit. An engineer is trying to block the route to 192.168.2.2 from the routing table by using the configuration that is shown. The route is still present in the routing table as an OSPF route. Which action blocks the route?

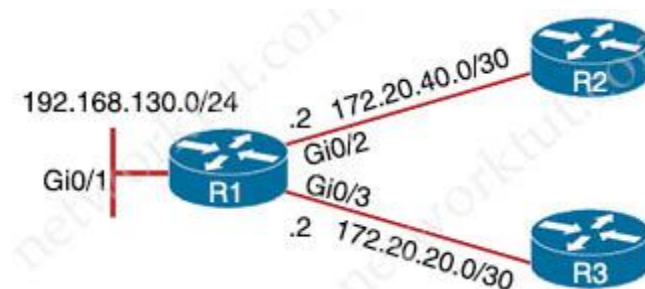
```
Router#show access-lists
Standard IP access list 1
  10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
network 192.168.1.1 0.0.0.0 area 0
network 192.168.12.0 0.0.0.255 area 0
distribute-list route-map RM-OSPF-DL in
Router#
```

- A. Add this statement to the route map “route-map RM-OSPF-DL deny 20”
- B. Use a prefix list instead of an access list in the route map
- C. Change sequence 10 in the route-map command from permit to deny
- D. Use an extended access list instead of a standard access list

**Answer: C**

### Question 3

Refer to the exhibit. Which configuration configures a policy on R1 to forward any traffic that is sourced from the 192.168.130.0/24 network to R2?



- A. access-list 1 permit 192.168.130.0 0.0.0.255
- !
- interface Gi0/2
- ip policy route-map test
- !
- route-map test permit 10
- match ip address 1
- set ip next-hop 172.20.20.2

B. access-list 1 permit 192.168.130.0 0.0.0.255  
!  
interface Gi0/2  
ip policy route-map test  
!  
route-map test permit 10  
match ip address 1  
set ip next-hop 172.20.20.1

C. access-list 1 permit 192.168.130.0 0.0.0.255  
!  
interface Gi0/1  
ip policy route-map test  
!  
route-map test permit 10  
match ip address 1  
set ip next-hop 172.20.40.2

D. access-list 1 permit 192.168.130.0 0.0.0.255  
!  
interface Gi0/1  
ip policy route-map test  
!  
route-map test permit 10  
match ip address 1  
set ip next-hop 172.20.40.1

E. access-list 1 permit 192.168.130.0 0.0.0.255  
!  
interface Gi0/1  
ip policy route-map test  
!  
route-map test permit 10  
match ip address 1  
set ip next-hop 172.20.20.1

**Answer: D**

## Redistribution Questions

<https://www.networktut.com/redistribution-questions>

### Question 1

Refer to the exhibit. Which statement about R1 is true?

R1 (config)#route-map ADD permit 20
-------------------------------------

```
R1 (config-route-map)#set tag 1
R1 (config)#router ospf 1
R1 (config-router)#redistribute rip subnets route-map ADD
```

- A. OSPF redistributes RIP routes only if they have a tag of one
- B. RIP learned routes are distributed to OSPF with a tag value of one
- C. R1 adds one to the metric for RIP learned routes before redistributing to OSPF
- D. RIP routes are redistributed to OSPF without any changes

**Answer: B**

### Question 2

Refer to the exhibit. Which routes from OSPF process 5 are redistributed into EIGRP?

```
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
```

- 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

**Answer: A**

### Question 3

Refer to Exhibit. Which statement about redistribution from BGP into OSPF process 10 is true?

```
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
```

- A. Network 172.16.1.0/24 is not redistributed into OSPF
- B. Network 10.10.10.0/24 is not redistributed into OSPF

- C. Network 172.16.1.0/24 is redistributed with administrative distance of 1
- D. Network 10.10.10.0/24 is redistributed with administrative distance of 20

**Answer: A**

#### Question 4

Which two statements about redistributing EIGRP into OSPF are true? (Choose two)

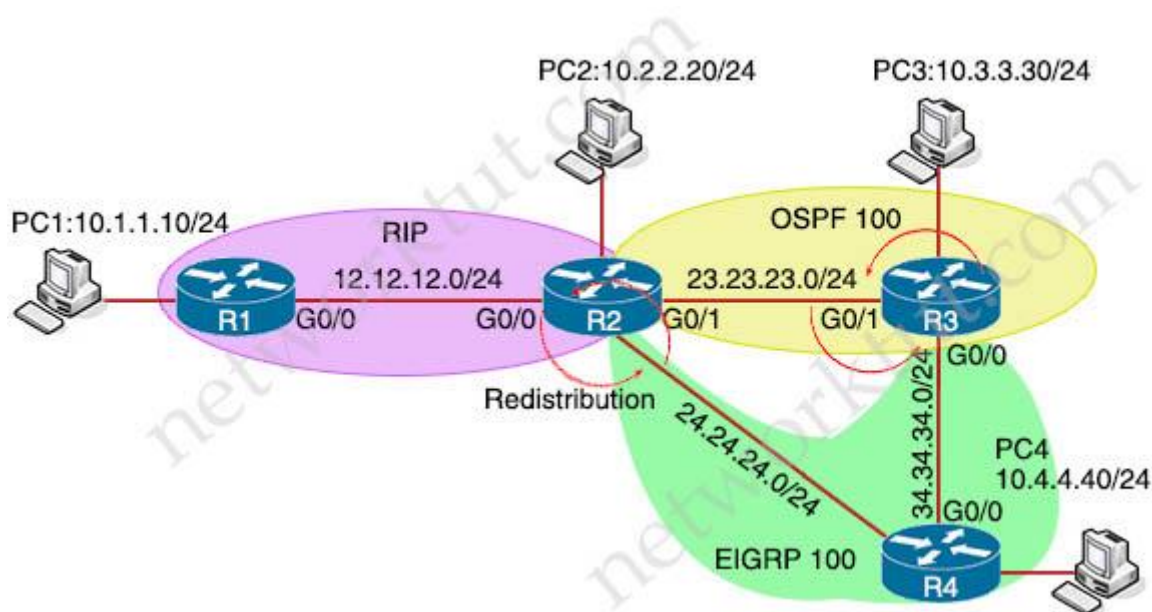
- A. The redistributed EIGRP routes appear as type 3 LSAs in the OSPF database
- B. The redistributed EIGRP routes appear as type 5 LSAs in the OSPF database
- C. The administrative distance of the redistributed routes is 170
- D. The redistributed EIGRP routes appear as OSPF external type 1
- E. The redistributed EIGRP routes are placed into an OSPF area whose area ID matches the EIGRP autonomous system number
- F. The redistributed EIGRP routes appear as OSPF external type 2 routes in the routing table

**Answer: B F**

#### Question 5

Refer to the exhibit. After redistribution is enabled between the routing protocols, PC2, PC3, and PC4 cannot reach PC1.

Which action can the engineer take to solve the issue so that all the PCs are reachable?



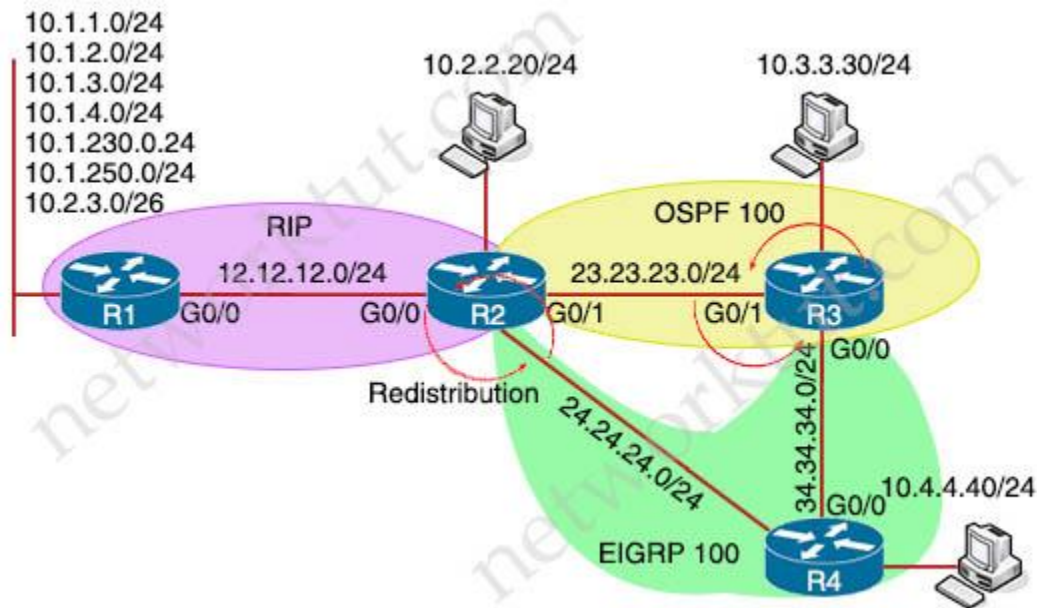
- A. Filter the prefix 10.1.1.0/24 when redistributed from OSPF to EIGRP.
- B. Set the administrative distance 100 under the process on R2.

- C. Filter the prefix 10.1.1.0/24 when redistributed from RIP to EIGRP.
- D. Redistribute the directly connected interfaces on R2.

**Answer: A**

### Question 6

Refer to the exhibit. Which subnet is redistributed from EIGRP to OSPF routing protocols?



```
R3
router ospf 100
 redistribute eigrp 100 subnets route-map OSPF-TAG-1

ip prefix-list OSPF-TAG-PRF seq 5 deny 10.1.0.0/16 le 24
!
ip prefix-list OSPF-TAG-PRF-1 seq 5 permit 10.2.0.0/18 le 24
!
route-map OSPF-TAG-1 deny 5
 match ip address prefix-list OSPF-TAG-PRF
 set tag 40
!
route-map OSPF-TAG-1 permit 10
 match ip address prefix-list OSPF-TAG-PRF-1
 set tag 80
!
```

- A. 10.2.2.0/24
- B. 10.1.4.0/24
- C. 10.1.2.0/24
- D. 10.2.3.0/26

Answer: A

### Question 7

Refer to the exhibit. An engineer is trying to redistribute OSPF to BGP, but not all of the routes are redistributed. What is the reason for this issue?

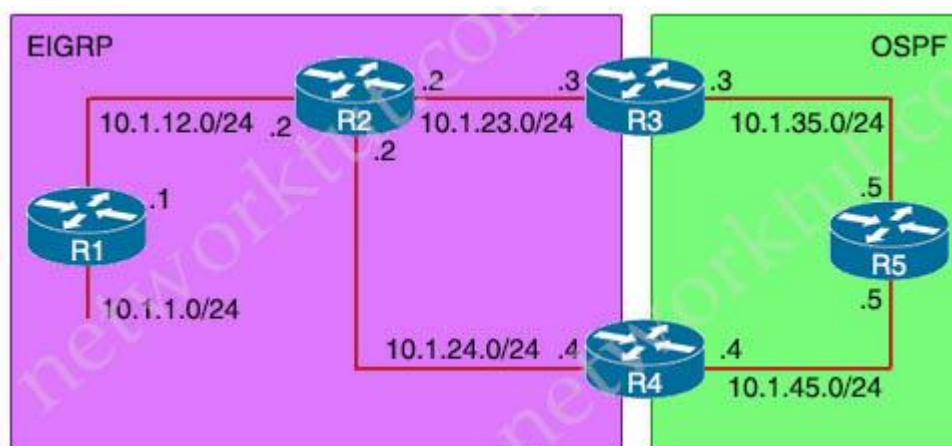
```
O E2      10.0.0.0 [110/20] via 192.168.12.2, 00:00:33, Ethernet0/0
O 192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:43, Ethernet0/0
Router#
Router#show ip bgp
--output omitted--
      Network                Next Hop           Metric LocPrf Weight Path
*> 192.168.1.1/32            0.0.0.0              0         32768 ?
*> 192.168.3.0               192.168.12.2         20         32768 ?
*> 192.168.12.0             0.0.0.0              0         32768 ?
Router#show running-config | section router bgp
router bgp 65000
  bgp log-neighbor-changes
  redistribute ospf 1
Router#
```

- A. By default, only internal OSPF routes are redistributed into BGP
- B. By default, only internal routes and external type 1 routes are redistributed into BGP
- C. BGP convergence is slow, so the route will eventually be present in the BGP table
- D. Only classful networks are redistributed from OSPF to BGP

Answer: A

### Question 8

Refer to the exhibit The output of the trace from R5 shows a loop in the network.



```
R1
router eigrp 1
redistribute connected
network 10.1.12.1 0.0.0.0
```

```
R5#traceroute 10.1.1.1
Type escape sequence to abort.
```

<hr/> R3 router ospf 1 redistribute eigrp 1 network 10.1.35.3 0.0.0.0 area 0 <hr/> R4 router eigrp 1 redistribute ospf 1 metric 2000000 1 255 1 1500 ! router ospf 1 network 10.1.45.4 0.0.0.0 area 0	Tracing the route to 10.1.1.1  1 10.1.35.3 80 msec 44 msec 20 msec 2 10.1.23.2 44 msec 104 msec 64 msec 3 10.1.24.4 44 msec 64 msec 40 msec 4 10.1.45.5 24 msec 40 msec 20 msec 5 10.1.35.3 92 msec 144 msec 147 msec 6 10.1.23.2 103 msec 77 msec 88 msec —output omitted—
--	---

Which configuration prevents this loop?

<b>Option A</b> R3 router ospf 1 redistribute eigrp 1 subnets route-map SET-TAG ! route-map SET-TAG permit 10 set tag 1  R4 router eigrp 1 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG ! route-map FILTER-TAG deny 10 match tag 1 ! route-map FILTER-TAG permit 20	<b>Option B</b> R3 router eigrp 1 redistribute ospf 1 subnets route-map SET-TAG ! route-map SET-TAG permit 10 set tag 1  R4 router eigrp 1 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG network 10.1.24.4 0.0.0.0 ! route-map FILTER-TAG deny 10 match tag 1 ! route-map FILTER-TAG permit 20
<b>Option C</b> R3 router ospf 1 redistribute eigrp 1 subnets route-map SET-TAG ! route-map SET-TAG permit 10 set tag 1  R4 router eigrp 1 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG ! route-map FILTER-TAG permit 10	<b>Option D</b> R3 router ospf 1 redistribute eigrp 1 subnets route-map SET-TAG ! route-map SET-TAG deny 10 set tag 1  R4 router eigrp 1 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG ! route-map FILTER-TAG deny 10



match tag 1	match tag 1
-------------	-------------

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

## MPLS Questions

<https://www.networktut.com/mpls-questions>

### Question 1

Which transport layer protocol is used to form LDP sessions?

- A. UDP
- B. SCTP
- C. TCP
- D. RDP

**Answer: C**

### Question 2

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**

### Question 3

Which command allows traffic to load-balance in an MPLS Layer 3 VPN configuration?

- A. Multi-paths eibgp 2
- B. Maximum-paths ibgp 2

- C. Multi-paths 2
- D. Maximum-paths 2

**Answer: D**

#### **Question 4**

Refer to the exhibit. What does the imp-null tag represent in the MPLS VPN cloud?

```
Router#show tag-switching tdp bindings
(...)
tib entry: 10.10.10.1/32, rev 31
  local binding: tag: 18
  remote binding: tsr: 10.10.10.1:0, tag:imp-null
  remote binding: tsr: 10.10.10.2:0, tag:18
  remote binding: tsr: 10.10.10.6:0, tag:21
tib entry: 10.10.10.2/32, rev 22
  local binding: tag: 17
  remote binding: tsr: 10.10.10.2:0, tag:imp-null
  remote binding: tsr: 10.10.10.1:0, tag:19
  remote binding: tsr: 10.10.10.6:0, tag:22
```

- A. Include the EXP bit
- B. Exclude the EXP bit
- C. Impose the label
- D. Pop the label

**Answer: D**

#### **Question 5**

Which list defines the contents of an MPLS label?

- A. 20-bit label; 3-bit traffic class; 1 -bit bottom stack; 8-bit TTL
- B. 32-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
- C. 20-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
- D. 32-bit label; 3-bit traffic class; 1 -bit bottom stack; 8-bit TTL

**Answer: A**

#### **Question 6**

What statement about route distinguishes in an MPLS network is true?

- A. Route distinguishers make a unique VPNv4 address across the MPLS network
- B. Route distinguishers allow multiple instances of a routing table to coexist within the edge

router

- C. Route distinguishers are used for label bindings
- D. Route distinguishers define which prefixes are imported and exported on the edge router

**Answer: A**

## VRF-Lite Questions

<https://www.networktut.com/vrf-lite-questions>

### Question 1

What is the output of the following command:

```
show ip vrf
```

- A. Shows default RD values
- B. Displays IP routing table information associated with a VRF
- C. Shows routing protocol information associated with a VRF
- D. Displays the ARP table (static and dynamic entries) in the specified VRF

**Answer: A**

### Question 2

Which protocol does VRF-Lite support?

- A. IS-IS
- B. ODR
- C. EIGRP
- D. IGRP

**Answer: C**

### Question 3

Which two statements about VRF-Lite configurations are true? (Choose two)

- A. They support the exchange of MPLS labels
- B. Different customers can have overlapping IP addresses on different VPNs
- C. They support a maximum of 512,000 routes
- D. Each customer has its own dedicated TCAM resources

- E. Each customer has its own private routing table
- F. They support IS-IS

**Answer:** B E

#### **Question 4**

What is the role of a route distinguisher via a VRF-Lite setup implementation?

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

**Answer:** A

#### **Question 5**

Which command displays the IP routing table information that is associated with VRF-Lite?

- A. show ip vrf
- B. show ip route vrf
- C. show run vrf
- D. show ip protocols vrf

**Answer:** B

#### **Question 6**

Which configuration enables the VRF that is labeled "inet" on FastEthernet0/0?

- A. R1(config)# ip vrf Inet  
R1(config-vrf)#ip vrf FastEthernet0/0
- B. R1 (conflg)#ip vrf Inet FastEthernet0/0
- C. R1(config)# ip vrf Inet  
R1(config-vrf)#interface FastEthernet0/0  
R1(config-if)#ip vrf forwarding Inet
- D. R1 (config)#router ospf 1 vrf Inet  
R1 (config-router)#ip vrf forwarding FastEthernet0/0

Answer: C

## DMVPN Questions

<https://www.networktut.com/dmvpn-questions>

### Question 1

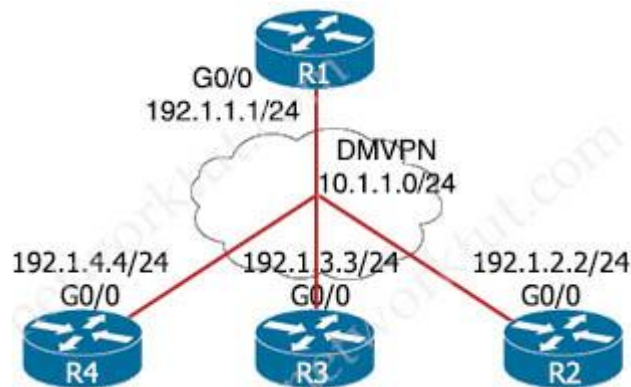
Which protocol is used to determine the NBMA address on the other end of a tunnel when mGRE is used?

- A. NHRP
- B. IPsec
- C. MP-BGP
- D. OSPF

Answer: A

### Question 2

Refer to the exhibits. Phase-3 tunnels cannot be established between spoke-to-spoke in DMVPN. Which two commands are missing? (Choose two)



On R2:  
R2(config)#interface tunnel 1  
R2(config-if)#ip address  
10.1.1.2 255.255.255.0  
R2(config-if)#tunnel source  
FastEthernet0/0  
R2(config-if)#tunnel mode gre  
multipoint  
R2(config-if)#ip nhrp network-

On R3:  
R3(config)#interface tunnel 1  
R3(config-if)#ip address  
10.1.1.3 255.255.255.0  
R3(config-if)#tunnel source  
FastEthernet0/0  
R3(config-if)#tunnel mode gre  
multipoint  
R3(config-if)#ip nhrp network-

On R4:  
R4(config)#interface tunnel 1  
R4(config-if)#ip address  
10.1.1.4 255.255.255.0  
R4(config-if)#tunnel source  
FastEthernet0/0  
R4(config-if)#tunnel mode gre  
multipoint  
R4(config-if)#ip nhrp network-

id 222 R2(config-if)#ip nhrp nhs 10.1.1.1 R2(config-if)#ip nhrp map 10.1.1.1 192.1.1.1	id 333 R3(config-if)#ip nhrp nhs 10.1.1.1 R3(config-if)#ip nhrp map 10.1.1.1 192.1.1.1	id 444 R4(config-if)#ip nhrp nhs 10.1.1.1 R4(config-if)#ip nhrp map 10.1.1.1 192.1.1.1
--	--	--

- A. The ip nhrp redirect command is missing on the spoke routers.
- B. The ip nhrp shortcut command is missing on the spoke routers.
- C. The ip nhrp redirect commands is missing on the hub router.
- D. The ip shortcut commands is missing on the hub router.
- E. The ip nhrp map command is missing on the hub router.

**Answer: B C**

### Question 3

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

**Answer: A**

### Question 4

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

**Answer: A**

**Question 5**

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

**Answer: D**

**Question 6**

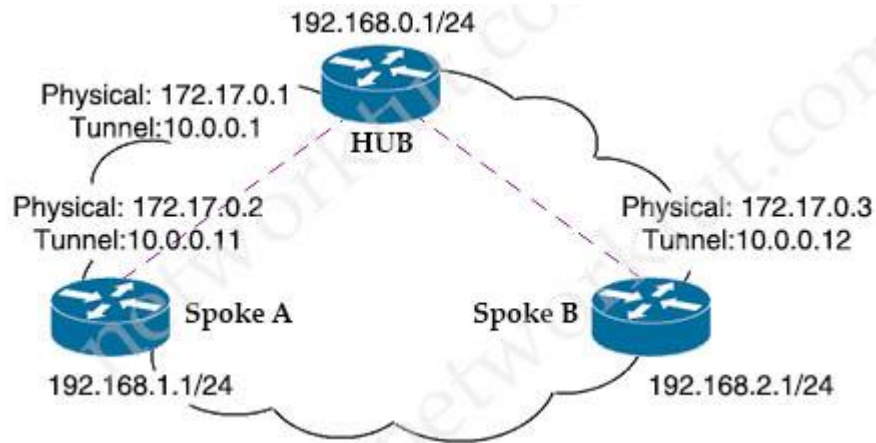
Which two methods use IPsec to provide secure connectivity from the branch office to the headquarters office? (Choose two)

- A. DMVPN
- B. MPLS VPN
- C. Virtual Tunnel Interface (VTI)
- D. SSL VPN
- E. PPPoE

**Answer: A C**

**Question 7**

Refer to the exhibit. Which interface configuration must be configured on the spoke A to enable a dynamic DMVPN tunnel with the spoke B router?



A. interface Tunnel0  
description mGRE – DMVPN Tunnel  
ip address 10.0.0.11 255.255.255.0  
ip nhrp map multicast dynamic  
ip nhrp network-id 1  
tunnel source 10.0.0.1  
tunnel destination FastEthernet0/0  
tunnel mode gre multipoint

B. interface Tunnel0  
ip address 10.1.0.11 255.255.255.0  
ip nhrp network-id 1  
tunnel source 1.1.1.10  
ip nhrp map 10.0.0.11 172.17.0.2  
tunnel mode gre

C. interface Tunnel0  
ip address 10.0.0.11 255.255.255.0  
ip nhrp map multicast static  
ip nhrp network-id 1  
tunnel source 10.0.0.1  
tunnel mode gre multipoint

D. interface Tunnel0  
ip address 10.0.0.11 255.255.255.0  
ip nhrp network-id 1  
tunnel source FastEthernet0/0  
tunnel mode gre multipoint  
ip nhrp nhs 10.0.0.1  
ip nhrp map 10.0.0.1 172.17.0.1

**Answer: D**

**Question 8**



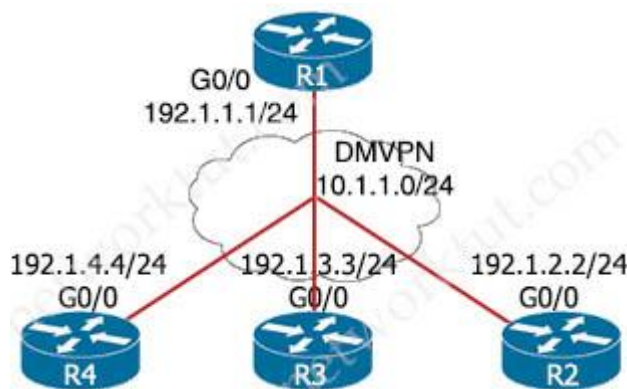
Which security feature can protect DMVPN tunnels?

- A. IPsec
- B. TACACS+
- C. RTBH
- D. RADIUS

**Answer: A**

### Question 9

Refer to the exhibit. After applying IPsec, the engineer observed that the DMVPN tunnel went down, and both spoke-to-spoke and hub were not establishing. Which two actions resolved the issue? (Choose two)



#### R2:

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#encryption 3des
R2(config)#crypto isakmp key cisco address
10.1.1.1
R2(config)#crypto ipsec transform-set TSET
esp-des esp-md5-hmac
R2(cfg-crypto-trans)#mode transport
R2(config)#crypto ipsec profile TST
R2(ipsec-profile)#set transform-set TSET
R2(config)#interface tunnel 123
E2(config-if)#tunnel protection ipsec profile
TST
```

#### R3:

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#hash md5
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#encryption 3des
R3(config)#crypto isakmp key cisco address
10.1.1.1
R3(config)#crypto ipsec transform-set TSET
esp-des esp-md5-hmac
R3(cfg-crypto-trans)#mode tunnel
R3(config)#crypto ipsec profile TST
R3(ipsec-profile)#set transform-set TSET
R3(config)#interface tunnel 123
R3(config-if)#tunnel protection ipsec profile
TST
```

- A. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3
- B. Remove the crypto isakmp key cisco address 10.1.1.1 on R2 and R3

- C. Change the mode from mode transport to mode tunnel on R2
- D. Configure the mode from mode tunnel to mode transport on R3

**Answer:** A B

## AAA Questions

<https://www.networktut.com/aaa-questions>

### Question 1

Refer to the exhibit. An engineer is trying to configure local authentication on the console line, but the device is trying to authenticate using TACACS+. Which action produces the desired configuration?

```
R1#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login Console local
R1#show running-config | section line
line con 0
logging synchronous
R1#
```

- A. Add the aaa authentication login default group tacacs+ local-case command to the global configuration
- B. Add the login authentication Console command to the line configuration
- C. Replace the capital “C” with a lowercase “c” in the aaa authentication login Console local command
- D. Add the aaa authentication login default none command to the global configuration

**Answer:** B

### Question 2

Refer to the exhibit. Why is user authentication being rejected?

```
TAC+: TCP/IP open to 171.68.118.101/49 failed —
Destination unreachable; gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (2546660185): status = FAIL
```

As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure

- A. The TACACS+ server expects “user” but the NT client sends “domain\user”
- B. The TACACS+ server refuses the user because the user is set up for CHAP
- C. The TACACS+ server is down and the user is in the local database
- D. The TACACS+ server is down and the user is not in the local database

**Answer: D**

## NTP Questions

<https://www.networktut.com/ntp-questions>

### Question 1

Refer to the exhibit. An administrator noticed that after a change was made on R1, the timestamps on the system logs did not match the clock. What is the reasons for this error?

```
service timestamps debug datetime msec
service timestamps log datetime
clock timezone MST -7 0
clock summer-time MST recurring
ntp authentication-key 1 md5 00101AOB0152181206224747071E 7
ntp server 10.10.10.10
```

**R1#show clock**

\*06:13:44.045 MST Sun Dec 30 2018

**R1#conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#logging host 10.10.10.20

R1(config)#end

R1#

\*Dec 30 13:15:26: %SYS-S-CONFIG\_I: Configured from console by console

R1#

\*Dec 30 13:18:28: %SYS-6-LOGGINGHOST\_STARTSTOP: Logging to host 10.10.10.20 port 514 started – CLI initiated

- A. The keyword localtime is not defined on the timestamp service command
- B. The NTP server is in an different time zone
- C. An authentication error with the NTP server results in an incorrect timestamp
- D. The system clock is set incorrectly to summer-time hours

**Answer: A**

## Question 2

Refer to the exhibit An engineer is troubleshooting BGP on a device but discovers that the clock on the device does not correspond to the time stamp of the log entries.

Which action ensures consistency between the two times?

```
*Feb 28 12:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Down User reset
*Feb 28 12:41:57: %BGP_SESSION-5-ADJCHANGE : neighbor 192.168.2.2 IPv4 Unicast
topology base removed from session User reset
*Feb 28 12:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Up
R1#show clock
*13:42:00.506 CET Feb 28 2019
```

- A. Configure the logging clock synchronize command in global configuration mode
- B. Configure the service timestamps log uptime command in global configuration mode
- C. Configure the service timestamps log datetime localtime command in global configuration mode
- D. Make sure that the clock on the device is synchronized with an NTP server

**Answer: C**

## Question 3

A network engineer is investigating a flapping (up/down) interface issue on a core switch that is synchronized to an NTP server. Log output does not show the time of the flap.

Which command allows on the switch the time of the flap according to the dock on the device?

- A. clock calendar-valid
- B. service timestamps log datetime localtime show-timezone
- C. service timestamps log uptime
- D. dock summer-time mst recurring 2 Sunday mar 2:00 1 Sunday nov 2:00

**Answer: B**

# Access-list Questions

<https://www.networktut.com/access-list-questions>

## Question 1

Refer to the exhibit. During troubleshooting it was discovered that the device is not reachable using a secure web browser. What is needed to fix the problem?

```
access-list 100 deny tcp any any eq 465
access-list 100 deny tcp any eq 465 any
```

```
access-list 100 permit tcp any any eq 80
access-list 100 permit tcp any eq 80 any
access-list 100 permit udp any any eq 443
access-list 100 permit udp any eq 443 any
```

- A. permit tcp port 465
- B. permit tcp port 443
- C. permit udp port 465
- D. permit tcp port 22

**Answer: B**

## Question 2

Refer to the exhibit. Which configuration denies Telnet traffic to router 2 from 198A:0:200C::1/64?



- A. 

```
ipv6 access-list Deny_Telnet
sequence 10 deny tcp host 198A:0:200C::1/64 host 201A:0:205C::1/64
!
int Gi0/0
ipv6 access-map Deny_Telnet in
!
```
- B. 

```
ipv6 access-list Deny_Telnet
sequence 10 deny tcp host 198A:0:200C::1/64 host 201A:0:205C::1/64
!
int Gi0/0
ipv6 traffic-filter Deny_Telnet in
!
```
- C. 

```
ipv6 access-list Deny_Telnet
sequence 10 deny tcp host 198A:0:200C::1/64 host 201A:0:205C::1/64 eq telnet
!
int Gi0/0
ipv6 access-map Deny_Telnet in
!
```
- D. 

```
ipv6 access-list Deny_Telnet
sequence 10 deny tcp host 198A:0:200C::1/64 host 201A:0:205C::1/64 eq telnet
!
```

```
int Gi0/0
ipv6 traffic-filter Deny_Telnet in
```

**Answer: D**

## Control Plane Questions

<https://www.networktut.com/control-plane-questions>

### Question 1

While troubleshooting connectivity issues to a router, these details are noticed:

- standard pings to all router interfaces, including loopbacks, are successful.
- Data traffic is unaffected.
- SNMP connectivity is intermittent.
- SSH is either or disconnects frequently.

Which command must be configured first to troubleshoot this issue?

- A. Show policy-map control-plane
- B. Show policy-map
- C. Show interface inc drop
- D. Show ip route

**Answer: A**

### Question 2

Refer to the exhibit. An engineer is trying to connect to a device with SSH but cannot connect. The engineer connects by using the console and find the displayed output when troubleshooting. Which command must be used in configuration mode to enable SSH on the device?

```
R1#show ip ssh
SSH Disabled — version 1.99
% Please create RSA keys to enable SSH (and of at least 768 bits for SSH v2).
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size: 1024 bits
IOS Keys in SECSH format (ssh-rsa, base64 encoded): NONE
R1#
```

- A. crypto key generate rsa
- B. ip ssh enable
- C. no ip ssh disable
- D. ip ssh version 2

**Answer: A**

### **Question 3**

Which option is the best for protecting CPU utilization on a device?

- A. fragmentation
- B. COPP
- C. ICMP redirects
- D. ICMP unreachable messages

**Answer: B**

### **Question 4**

An engineer is trying to copy an IOS file from one router to another router by using TFTP. Which two actions are needed to allow the file to copy? (Choose two)

- A. Configure the TFTP authentication on the source router with the “tftp-server authentication local” command.
- B. Configure a user on the source router with the username tftp password tftp command.
- C. Enable the TFTP server on the source router with the tftp-server flash:<filename> command.
- D. TFTP is not supported in recent IOS versions, so an alternative method must be used.
- E. Copy the file to the destination router with the copy tftp: flash: command

**Answer: C E**

## **IPv6 Questions**

<https://www.networktut.com/ipv6-questions>

### **Question 1**

Which is statement about IPv6 inspection is true?

- A. It learns and secures bindings for stateless autoconfiguration addresses in Layer 3 neighbor tables
- B. It learns and secures bindings for stateful autoconfiguration addresses in Layer 3 neighbor tables
- C. It learns and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables
- D. It learns and secures binding for stateless autoconfiguration addresses in Layer 2 neighbor tables

**Answer: D**

### **Question 2**

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**

## **IP SLA Questions**

<https://www.networktut.com/ip-sla-questions>

### **Question 1**

Which command is used to check IP SLA when an interface is suspected to receive lots of traffic with options?

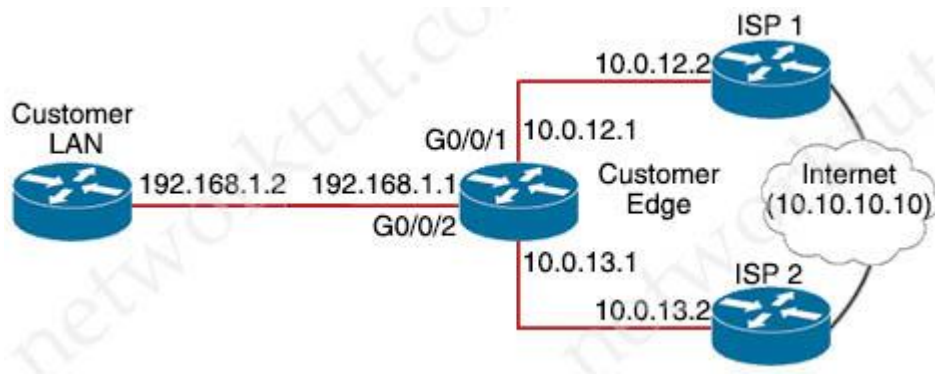
- A. show track
- B. show threshold
- C. show timer
- D. show delay

**Answer: A**

### **Question 2**

Refer to the exhibit. ISP 1 and ISP 2 directly connect to the internet. A customer is tracking both ISP links to achieve redundancy and cannot see the Cisco IP SLA tracking output on the router console. Which command is missing from the IP SLA configuration?





- A. Start-time now
- B. Start-time 00:00
- C. Start-time 0
- D. Start-time immediately

**Answer: A**

### Question 3

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?

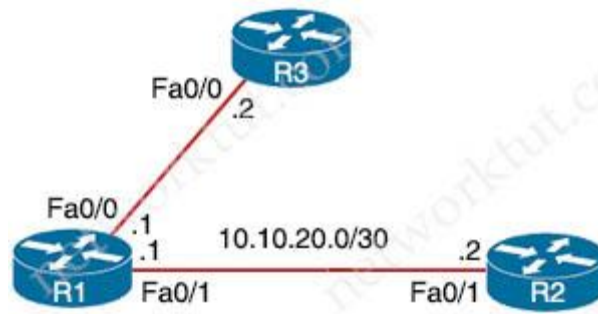
- A. show frequency
- B. show track
- C. show reachability
- D. show threshold

**Answer: B**

### Question 4

Refer to the exhibit. An IP SLA was configured on router R1 that allows the default route to be modified in the event that Fa0/0 losses reachability with the router R3 Fa0/0 interface. The route has changed to flow through route R2.

Which debug command is used to troubleshoot this issue?



- A. debug ip flow
- B. debug ip sla error
- C. debug ip routing
- D. debug ip packet

**Answer: C**

## SNMP Questions

<https://www.networktut.com/snmp-questions>

### Question 1

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

**Answer: B**

### Question 2

Refer to the exhibit. Network operations cannot read or write an configuration on the device with this configuration from the operation subnet. Which two configuration fix the issue? (Choose two)

```
snmp-server community ciscotest 1
snmp-server host 192.168.1.128 ciscotest
snmp-server enable traps bgp
```

- A. Configure SNMP rw permission in addition to community ciscotest
- B. Modify access list 1 and allow operations subnet in the access list
- C. Modify SNMP rw permission in addition to version 1
- D. Configure SNMP rw permission in addition to version 1
- E. Configure SNMP rw permission in addition to community ciscotest 1

**Answer:** A B

## DHCP Questions

<https://www.networktut.com/dhcp-questions>

### Question 1

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. Auto-QoS is blocking DHCP traffic
- B. The DHCP server IP address configuration is missing locally
- C. 802.1X is blocking DHCP traffic
- D. The broadcast domain is too large for proper DHCP propagation
- E. The route to the new DHCP server is missing

**Answer:** B E

### Question 2

Refer to the exhibit. Users report that IP addresses cannot be acquired from the DHCP server. The DHCP server is configured as shown. About 300 total nonconcurrent users are using this DHCP server, but none of them are active for more than two hours per day.

Which action fixes the issue within the current resources?

```
R1#show running-config | section dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp pool DHCP
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 8.8.8.8
  lease 0 12
```

- A. Configure the DHCP lease time to a bigger value
- B. Add the network 192.168.2.0 255.255.255.0 command to the DHCP pool
- C. Modify the subnet mask to the network 192.168.1.0 255.255.254.0 command in the DHCP

pool

D. Configure the DHCP lease time to a smaller value

**Answer: D**

## DNA Center Questions

<https://www.networktut.com/dna-center-questions>

### Question 1

An engineer configured the wrong default gateway for the Cisco DNA center enterprise interface during the install. Which command must the engineer run to correct the configuration?

- A. Sudo update config install
- B. Sudo maglev reinstall
- C. Sudo maglev-config update
- D. Sudo maglev install config update

**Answer: C**

### Question 2

When provisioning a device in Cisco DNA Center, the engineer sees the error message "Cannot select the device. Not compatible with template.". What is the reason for the error?

- A. The software version of the template is different from the software version of the device
- B. The changes to the template were not committed
- C. The template has an incorrect configuration
- D. The tag that was used to filter the templates does not match the device tag

**Answer: D**

### Question 3

While working with software images, an engineer observes that Cisco DNA Center cannot upload its software image directly from the device. Why is the image not uploading?

- A. The device has lost connectivity to Cisco DNA Center
- B. The software image for the device is in bundle mode

- C. The software image for the device is in install mode
- D. The device must be resynced to Cisco DNA Center

**Answer: C**

## Drag Drop Questions

<https://www.networktut.com/drag-drop-questions>

### Question 1

Drag and drop the MPLS VPN concepts from the left onto the correct descriptions on the right.

route distinguisher	propagates VPN reachability information
route target	distributes labels for traffic engineering
Resource Reservation Protocol	uniquely identifies a customer prefix
multiprotocol BGP	controls the import/export of customer prefixes

**Answer:**

- + propagates VPN reachability information: multiprotocol BGP
- + distributes labels for traffic engineering: Resource Reservation Protocol
- + uniquely identifies a customer prefix: route distinguisher
- + controls the import/export of customer prefixes: route target

### Question 2

Drag and drop the address from the left onto the correct IPv6 filter purposes on the right.

permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443	permit NTP from this source 2001:0D8B:0800:200c::1f
permit ip 2001:d8b:800:200c::e/126 2001:0D88:800:2010::/64 eq 514	permit syslog from this source 2001:0D88:0800:200c::1c
permit ip 2001:d8b:800:200c::800/117 2001:0DBB:800:2010::/64 eq 80	permit HTTP from this source 2001:0D8B:0800:200c::0fff
permit ip 2001:d88:800:200c::c/126 2001:0DBB:800:2010::/64 eq 123	permit HTTPS from this source 2001:0D8B:0800:200c::07ff

**Answer:**

+ permit NTP from this source 2001:0D88:0800:200c::1f – **permit ip 2001:d88:800:200c::c/126 2001:0DBB:800:2010::/64 eq 123**  
+ permit syslog from this source 2001:0D88:0800:200c::1c – **permit ip 2001:D88:800:200c::e/126 2001:0DBB:800:2010::/64 eq 514**  
+ permit HTTP from this source 2001:0D8B:0800:200c::0fff – **permit ip 2001:d8b:800:200c::800/117 2001:0DBB:800:2010::/64 eq 80**  
+ permit HTTPS from this source 2001:0D8B:0800:200c::07ff – **permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443**

### Question 3

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

data plane packets	user-generated packets that are always forwarded by network devices to other end-station devices
control plane packets	network device generated or received packets that are used for the creation of the network itself
management plane packets	network device generated or received packets; packets that are used to operate the network
services plane packets	user-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than the normal traffic by the network devices

**Answer:**

- + user-generated packets that are always forwarded by network devices to other end-station devices: **data plane packets**
- + network device generated or received packets that are used for the creation of the network itself: **control plane packets**
- + network device generated or received packets; packets that are used to operate the network: **management plane packets**
- + user-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than the normal traffic by the network devices: **services plane packets**

#### Question 4

Drag and drop the SNMP attributes in Cisco IOS devices from the onto the correct SNMPv2c or SNMPv3 categories on the right.

community string	SNMPv2c
username and password	
authentication	
no encryption	
privileged	SNMPv3
read-only	

**Answer:**

**SNMPv2c:**

- + community string
- + no encryption
- + read-only

**SNMPv3:**

- + username and password
- + authentication
- + privileged

#### Question 5



Drag and drop the MPLS terms from the left onto the correct definitions on the right.

PE	device that forwards traffic based on labels
P	path that the labeled packet takes
CE	device that is unaware of MPLS labeling
LSP	device that removes and adds the MPLS labeling

**Answer:**

- + device that forwards traffic based on labels: P
- + path that the labeled packet takes: LSP
- + device that is unaware of MPLS labeling: CE
- + device that removes and adds the MPLS labeling: PE

### Question 6

Drag and drop the OSPF adjacency states from the left onto the correct descriptions on the right

Init	Each router compares the DBD packets that were received from the other router
2-way	Routers exchange information with other routers in the multiaccess network
Down	The neighboring router requests the other routers to send missing entries
Exchange	The network has already elected a DR and a backup BDR
ExStart	The OSPF router ID of the receiving router was not contained in the hello message
Loading	No hellos have been received from a neighbor router

**Answer:**

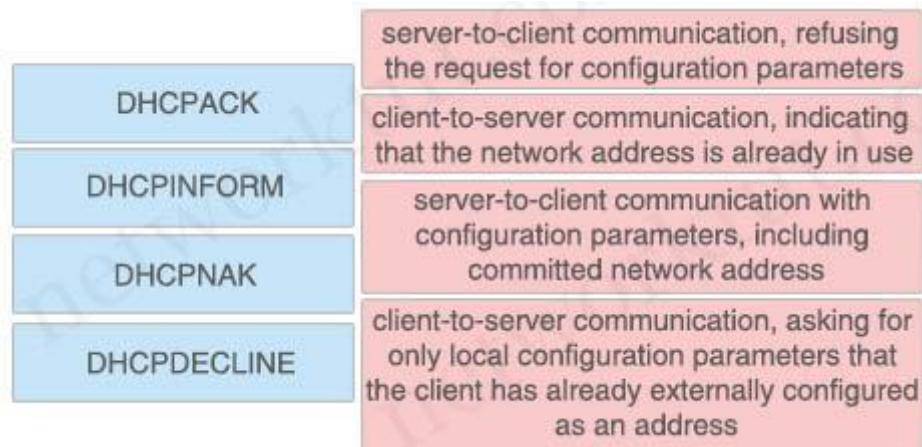
- + Each router compares the DBD packets that were received from the other router: Exchange
- + Routers exchange information with other routers in the multiaccess network: 2-way



- + The neighboring router requests the other routers to send missing entries: Loading
- + The network has already elected a DR and a backup BDR: Exstart
- + The OSPF router ID of the receiving router was not contained in the hello message: Init
- + No hellos have been received from a neighbor router: Down

### Question 7

Drag and drop the DHCP messages from the left onto the correct uses on the right.



### Answer:

- + server-to-client communication, refusing the request for configuration parameters: DHCPNAK
- + client-to-server communication, indicating that the network address is already in use: DHCPDECLINE
- + server-to-client communication with configuration parameters, including committed network address: DHCPACK
- + client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address: DHCPINFORM

## Miscellaneous Questions

<https://www.networktut.com/miscellaneous-questions>

### Question 1

What is a prerequisite for configuring BFD?

- A. All routers in the path between two BFD endpoints must have BFD enabled
- B. Jumbo frame support must be configured on the router that is using BFD
- C. Cisco Express Forwarding must be enabled on all participating BFD endpoints
- D. To use BFD with BGP, the timers 3 9 command must first be configured in the BGP routing process

**Answer: C**

### **Question 2**

Which two protocols can cause TCP starvation? (Choose two)

- A. TFTP
- B. SNMP
- C. SMTP
- D. HTTPS
- E. FTP

**Answer: A B**

### **Question 3**

Which method changes the forwarding decision that a router makes without first changing the routing table or influencing the IP data plane?

- A. Policy-based routing
- B. Nonbroadcast multi-access
- C. Packet switching
- D. Forwarding information base

**Answer: A**

### **Question 4**

Which attribute eliminates LFAs that belong to protected paths in situations where links in a network are connected through a common fiber?

- A. Interface-disjoint
- B. Shared risk link group-disjoint
- C. Linecard-disjoint
- D. Lowest-repair-path-metric

**Answer: B**

### **Question 5**

Refer to the exhibit. An administrator that is connected to the console does not see debug messages when remote users log in. Which action ensures that debug messages are displayed for remote loggings?

```
R1(config)#do show running-config | section line|username
username cisco secret 5 $!$^e/o$I3G5cXODxpYMSJ70PzEyoO
line con 0
logging synchronous
line vty 0 4
login local
transport input telnet
R1(config)# logging console 7
R1(config)# do debug aaa authentication
R1(config)#
```

- A. Enter the transport input ssh configuration command
- B. Enter the terminal monitor exec command
- C. Enter the logging console debugging configuration command
- D. Enter the aaa new-model configuration command

**Answer: D**

Refer to the exhibit. Why is the remote NetFlow server failing to receive the NetFlow data?

```
config t

flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 90
exit
!
flow monitor FLOW-MONITOR-1
record v4_r1
exit
!
ip cef
```

!

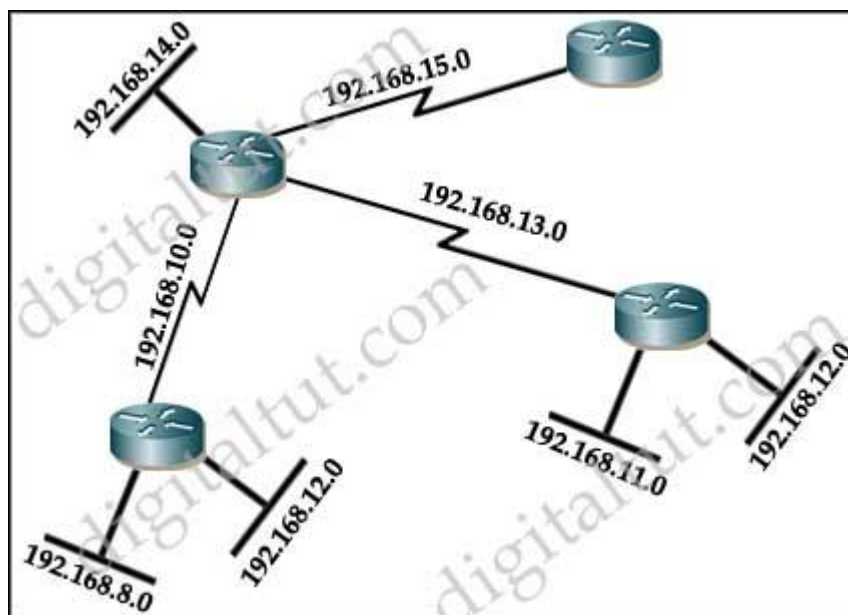
```
interface Ethernet0/0.1
ip address 172.16.6.2 255.255.255.0
ip flow monitor FLOW-MONITOR-1 input
```

- A. The flow exporter is configured but is not used.
- B. The flow monitor is applied in the wrong direction.
- C. The flow monitor is applied to the wrong interface.
- D. The destination of the flow exporter is not reachable.

**Answer: A**

### Question 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**