Taken on 7th Sep

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

- [x] LDP
- [x] RSVP
- [ ] MPLS OAM
- [ ] ECMP
- [ ] LSP

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?

- OSPF priority to 0
- tunnel interface of the hub with ip nhrp ospf dr
- (•) OSPF priority greater than 1
- route map to set the metrics of learned routes to 110

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?

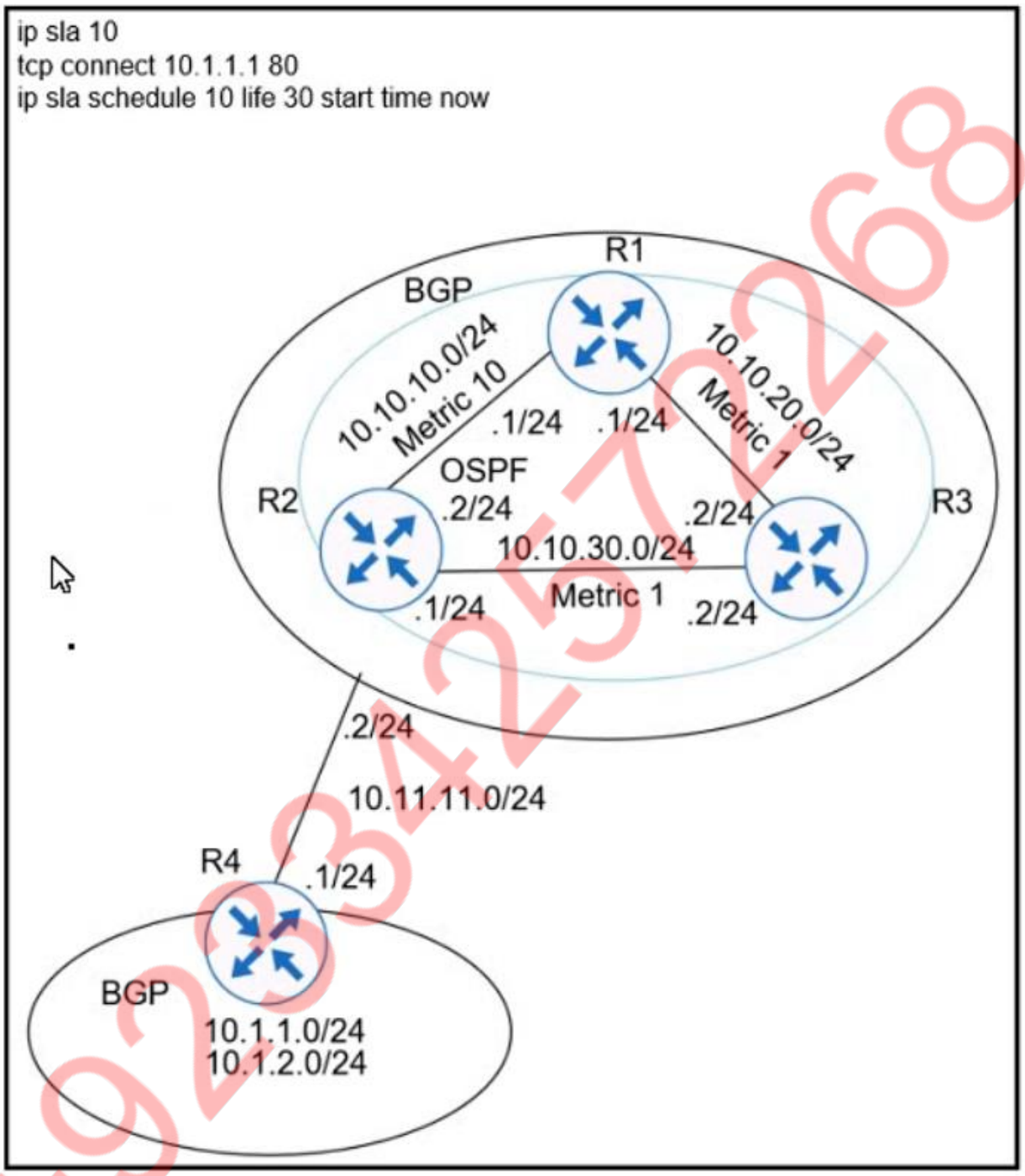
- (•) **ip verify unicast source reachable-via any**
- **ip verify unicast source reachable-via l2-src**
- **ip verify unicast source reachable-via allow-default**
- **ip verify unicast source reachable-via rx**

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

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

+923342572268

Taken on 7th Sep



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?

- Add the **control disable** option to the tcp connect.
- Modify the **ip sla schedule frequency** to forever.
- Re-issue the **ip sla schedule** command.
- Add **icmp-echo** command for the host.

+923425722268

Taken on 7th Sep

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 K0AyUubDrfOgO4s
authorization exec VTY_AUTH
login authentication VTY_AUTH

!
```

Debug Output:

```
AAA/AUTHEN/LOGIN (000004B6): Pick method list 'default'
AAA/AUTHOR (0x4B6): Pick method list 'VTY_AUTH'
AAA/AUTHOR/EXEC(000004B6): Authorization FAILED
```

Refer to the exhibit. Which action resolves the failed authentication attempt to the router?

- Configure **aaa authorization login** command on **line vty 0 4**.
- (•) Configure **aaa authorization console** global command.
- Configure **aaa authorization console** command on **line vty 0 4**.
- Configure **aaa authorization login** command on **line console 0**.

How does an MPLS Layer 3 VPN function?

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

+923342572268

Taken on 7th Sep

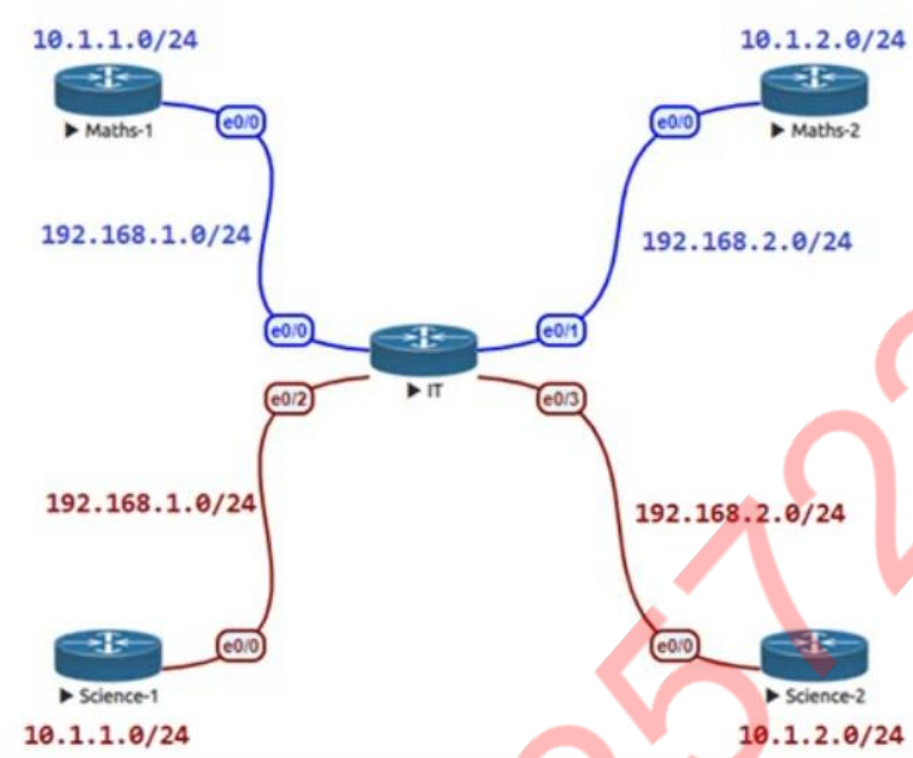
```
policy-map COPP-7600
 class COPP-CRITICAL-7600
  police cir 2000000 bc 62500
  conform-action transmit
  exceed-action transmit
  !
 class class-default
  police cir 200000 bc 6250
  conform-action transmit
  exceed-action drop
!
class-map match-all COPP-CRITICAL-7600
  match access-group name COPP-CRITICAL-7600
!
ip access-list extended COPP-CRITICAL-7600
  permit ip any any eq http
  permit ip any any eq https
```

+923342572268

Refer to the exhibit. BGP is flapping after the CoPP policy is applied. What are the two solutions to fix the issue? (Choose two.)

- [x] Configure a higher value for CIR under the default class to allow more packets during peak traffic.
- [ ] Configure a higher value for CIR under the **Class COPP-CRITICAL-7600**.
- [x] Configure BGP in the **COPP-CRITICAL-7600** ACL.
- [ ] Configure a three-color policer instead of two-color policer under **Class COPP-CRITICAL-7600**.
- [ ] Configure IP CEF for CoPP policy and BGP to work.

Taken on 7th Sep



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?

```
vrf definition Science
 address-family ipv4
!
interface E 0/2
 ip address 192.168.1.1 255.255.255.0
 no shut
!
interface E 0/3
 ip address 192.168.2.1 255.255.255.0
 no shut
```

```
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
```

```
vrf definition Science
 address-family ipv4
!
interface E 0/2
 ip address 192.168.1.1 255.255.255.0
 vrf forwarding Science
 no shut
!
interface E 0/3
 ip address 192.168.2.1 255.255.255.0
 vrf forwarding Science
 no shut
```

+923342572268

Taken on 7th Sep

```
vrf definition Science
 address-family ipv4
!
interface E 0/2
 ip address 192.168.1.1 255.255.255.0
 vrf forwarding Science
 no shut
!
interface E 0/3
 ip address 192.168.2.1 255.255.255.0
 vrf forwarding Science
 no shut
```

Answer is Option 2 which is B

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?

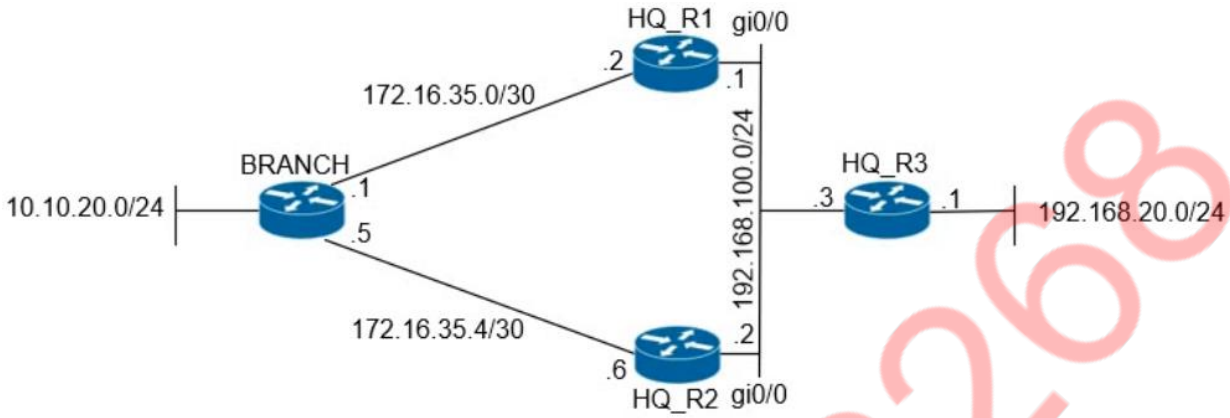
- BOOTP port 67
- DHCP option 66
- BOOTP port 68
- DHCP option 69

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?

- AS-PATH
- WEIGHT
- LOCAL_PREF
- MED

+923342572268

Taken on 7th Sep




```
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
```

Refer to the exhibit. 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?

- HQ_R3(config)# **ip sla responder**
  HQ_R3(config)# **ip sla responder icmp-echo 172.16.35.1**
- BRANCH(config)# **ip sla 1**
  BRANCH(config-ip-sla)# **icmp-echo 192.168.100.2**
- HQ_R3(config)# **ip sla responder**
  HQ_R3(config)# **ip sla responder icmp-echo 172.16.35.5**
- BRANCH(config)# **ip sla 1**
  BRANCH(config-ip-sla)# **icmp-echo 192.168.100.1**

+923425772268

Taken on 7th Sep

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

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

entropy label

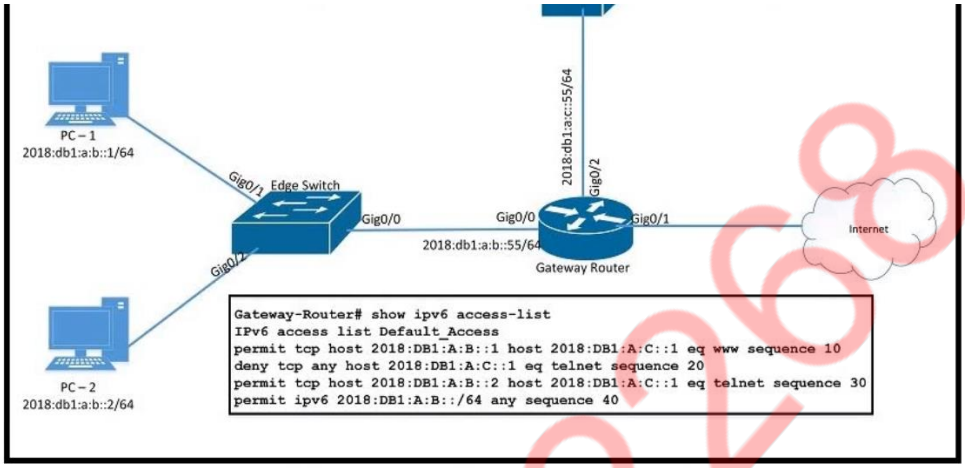
implicit null label

explicit null label

inbound label binding filtering

+923342572268

Taken on 7th Sep



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

- 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**
- 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**
- Gateway-Router(config)#**ipv6 access-list Default_Access**
  Gateway-Router(config-ipv6-acl)#**permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**
- 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**

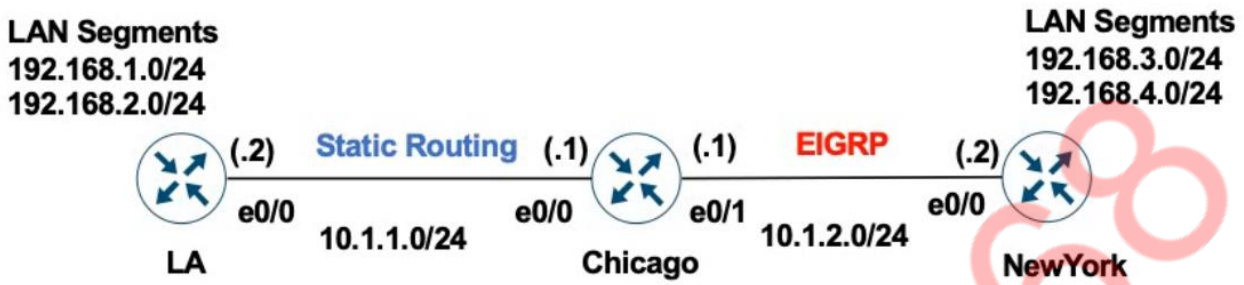
```
Jan 9 15:29:29.713: DHCP_SNOOPING: process new DHCP packet, message type: DHCPINFORM, input interface:
Po2, MAC da: ffff.ffff.ffff, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0
Jan 9 15:29:29.713: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is
flooded to ingress VLAN: (1)
Jan 9 15:29:29.722: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Vl1 for pak. Was Po2
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1Jan 9
15:29:31.517: DHCP_SNOOPING: received new DHCP packet from input interface (Port-channel2)
```

Refer to the exhibit. 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?

- **ip dhcp snooping**
- **ip dhcp relay information trust portchannel2**
- **ip dhcp snooping trust**
- **no ip dhcp snooping information option**

+923042572268

Taken on 7th Sep



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
```

Refer to the exhibits. 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?

- 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

- 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

- Chicago Router

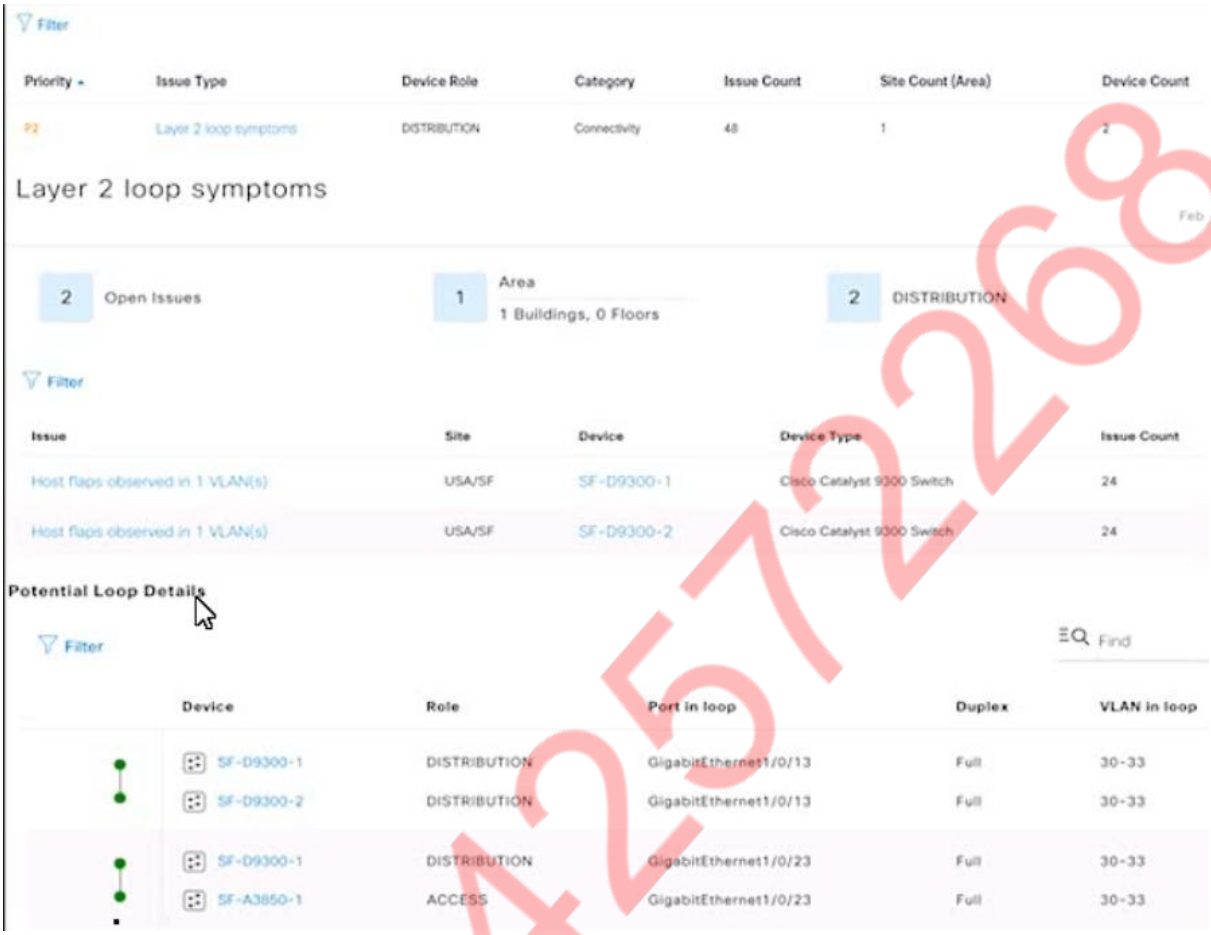
  router eigrp 100
  redistribute connected

- Chicago Router

  router eigrp 100
  redistribute static metric 10 10 10 10 10

+923342572268

Taken on 7th Sep



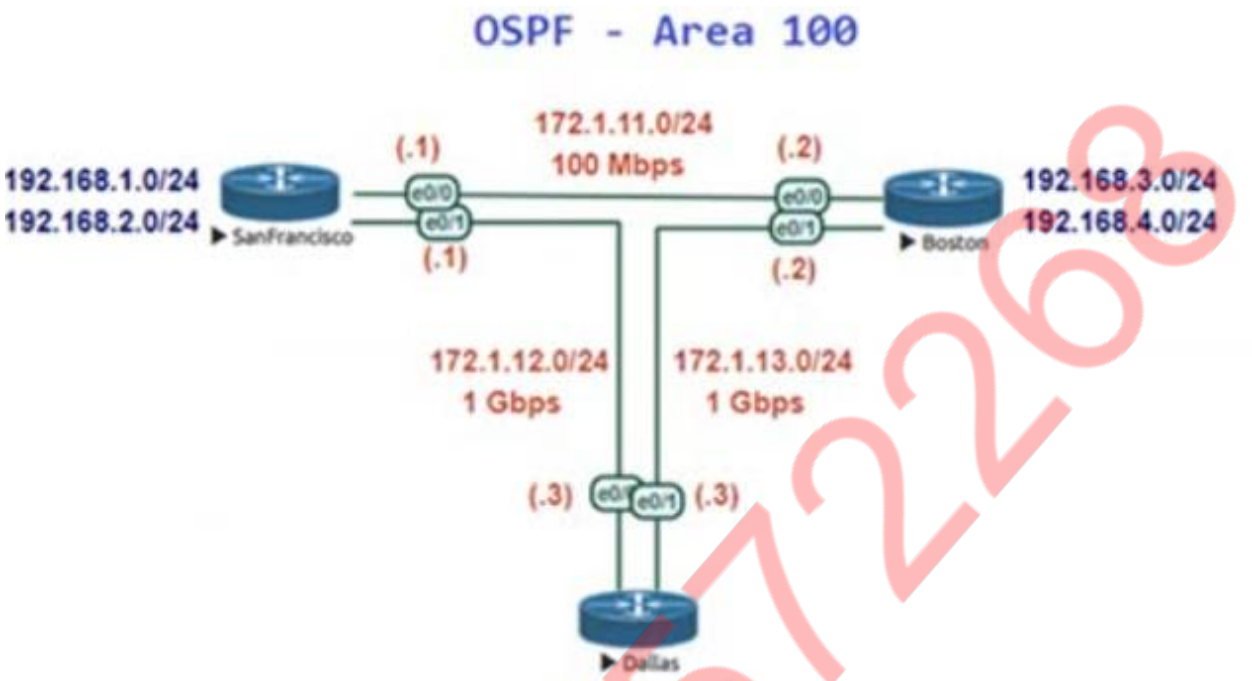

```
interface GigabitEthernet1/0/13
  switchport trunk allowed vlan 30-33
  switchport mode trunk
!
interface GigabitEthernet1/0/23
  switchport trunk allowed vlan 30-33
  switchport mode trunk
```

Refer to the exhibits. An engineer identified a Layer 2 loop using DNAC. Which command fixes the problem in the SF-D9300-1 switch?

- spanning-tree backbonefast
- spanning-tree loopguard default
- no spanning-tree uplinkfast
- spanning-tree portfast bpduguard

+923342572268

Taken on 7th Sep




```
     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, Ethernet0/0
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
```

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

- All Routers

```
router ospf 1
 auto-cost reference-bandwidth 100
```

- Boston Router

```
router ospf 1
 auto-cost reference-bandwidth 1000
```

- SanFrancisco Router

```
router ospf 1
 auto-cost reference-bandwidth 1000
```

- All Routers

```
router ospf 1
 auto-cost reference-bandwidth 1000
```

+923335972268

Taken on 7th Sep

Refer to the exhibit. 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?

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

  route-map SETLP permit 10
  match ip address prefix-list PLIST1
  set local-preference 110
  route-map SETLP permit 20

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

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

end

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

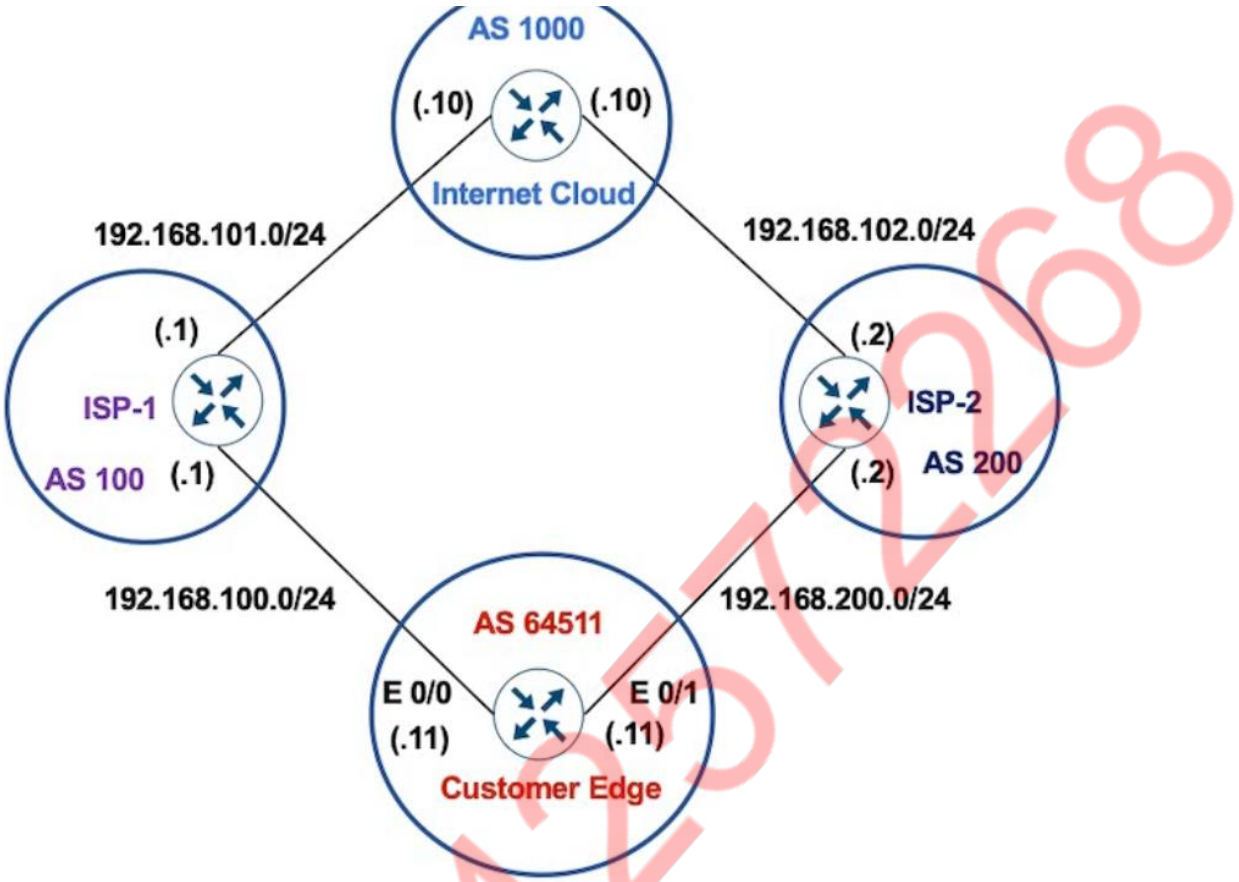
Network	Next Hop	Metric	LocPrf	Weight	Path
*> 2.2.2.0/24	0.0.0.0	0		32768	?
*> 131.108.1.0/24	2.2.2.2	84		32768	?
*> 131.108.2.0/24	2.2.2.2	74		32768	?

Refer to the exhibit. 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?

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

+923342712268

Taken on 7th Sep



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?

```
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
```

```
router bgp 64511
 aggregate-address 172.16.20.0 255.255.252.0 summary-only
```

```
interface E 0/0
 ip bgp suppress-map BLOCK_SPECIFIC
!
interface E 0/1
 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
```

```
router bgp 64511
 neighbor 192.168.100.1 summary-only
 neighbor 192.168.200.2 summary-only
```

1923425172268

Taken on 7th Sep

```
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
!
```

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

- 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.
- The OSPF process must have a metric when redistributing prefixes from EIGRP.
- EIGRP must redistribute the 10.0.106.0/24 route instead of using the network statement.
- The route map must have the keyword prefix-list to evaluate the prefix list entries.




```
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
```

Refer to the exhibit. Which configuration allows spoke-to-spoke communication using loopback as a tunnel source?

- Configure **crypto isakmp key cisco address 0.0.0.0** on the hub.
- Configure **crypto isakmp key cisco address 200.1.0.0 255.255.0.0** on the hub.
- Configure **crypto isakmp key cisco address 200.1.0.0 255.255.0.0** on the spokes.
- Configure **crypto isakmp key cisco address 0.0.0.0** on the spokes.

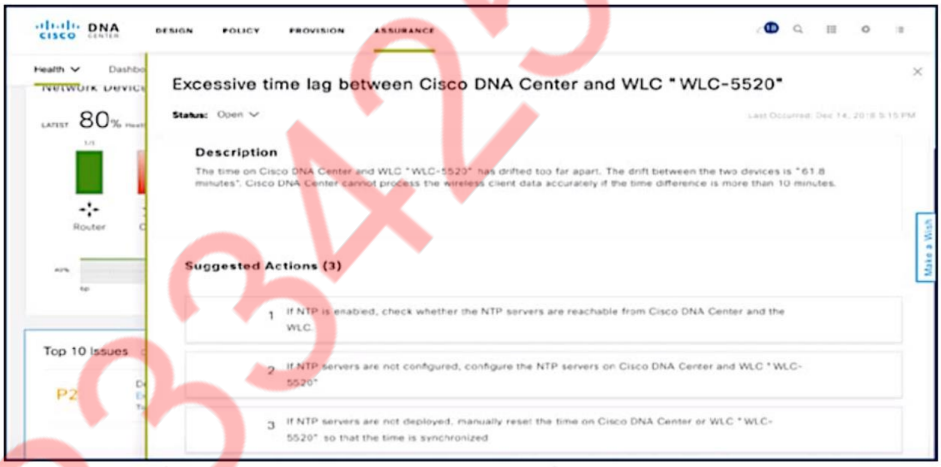
+923342572268

Taken on 7th Sep

```
      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 192.168.12.2, 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
```

Refer to the exhibits. All the serial links between R1, R2, and R3 have the same bandwidth. Users on the 192.168.1.0/24 network report slow response times while they access resources 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 do to fix the slowness?

- Redistribute the R1 static route to EIGRP.
- Remove the static route on R1.
- Change the Administrative Distance of EIGRP to 5.
- Add a static route on R1 using the next hop of R3.



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?

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

+923425572268

Taken on 7th Sep

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

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

```
 transport preferred telnet
 transport output none
 stopbits 0 4
line vty 0 4
 login
 transport referred telnet
 transport input none
 transport output telnet
R1#

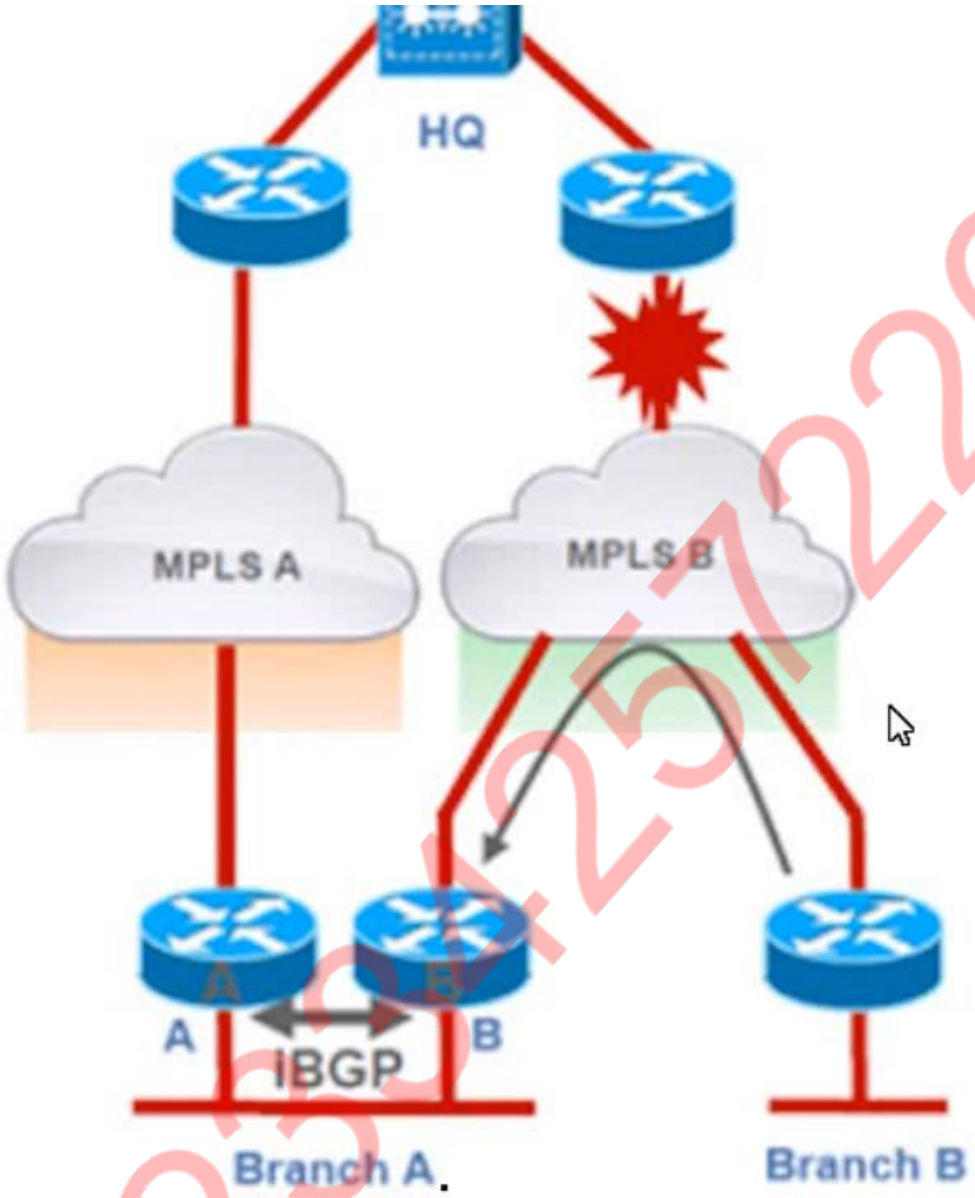
R1#ssh -1 cisco 192.168.12.2
% ssh connections not permitted from this terminal
R1#
```

Refer to the exhibit. An engineer receives this error message when trying to access another router in-band from the serial interface connected to the console of R1. Which configuration is needed on R1 to resolve this issue?

- R1(config)#**line console 0**
  R1(config-line)# **transport preferred ssh**
- 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**
- R1(config)#**line vty 0**
  R1(config-line)# **transport output ssh**

+923342572268

Taken on 7th Sep



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?

- 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.
- 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.
- Introduce an AS path filter on branch A routers so that only local prefixes are advertised into BGP.
- 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.

+923425722268

Taken on 7th Sep

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

- Configure all devices for SNMPv3 informs with auth.
- Configure all devices for SNMPv3 traps with auth.
- Configure all devices for SNMPv3 traps with priv.
- Configure all devices for SNMPv3 informs with priv.

```
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
```

Refer to the exhibit. When monitoring an IPv6 access list, an engineer notices that the ACL does not have any hits and is causing unnecessary traffic to pass through the interface. Which command must be configured to resolve the issue?

- **access-class INTERNET in**
- **ip access-group INTERNET in**
- **ipv6 traffic-filter INTERNET in**
- **ipv6 access-class INTERNET in**

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:

Head Office & Site A

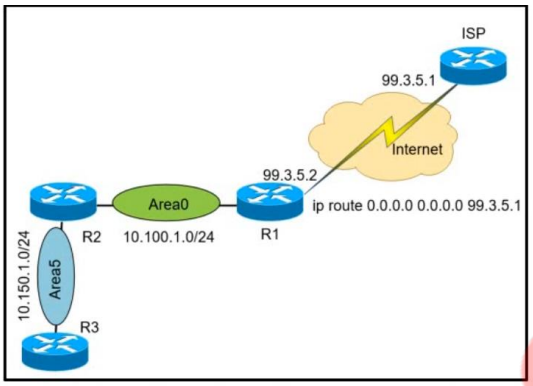
```
ip cef
ip vrf abc
rd 101:101
!
interface FastEthernet0/0
ip vrf forwarding abc
ip address 172.16.16.X 255.255.255.252
!
router ospf 1 vrf abc
log-adjacency-changes
network 172.16.16.0 0.0.0.255 area 1
```

After finishing both site router configurations, none of the LSA 3, 4, 5, and 7 are installed at Site A router. Which configuration resolves this issue?

- configure **capability vrf-lite** on Head Office and its connected PE router under **router ospf 1 vrf abc**
- configure **capability vrf-lite** on Site A and its connected PE router under **router ospf 1 vrf abc**
- configure **capability vrf-lite** on both PE routers connected to Head Office and Site A routers under **router ospf 1 vrf abc**
- configure **capability vrf-lite** on Head Office and Site A routers under **router ospf 1 vrf abc**

+923342572268

Taken on 7th Sep



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?

- router ospf 1
  network 0.0.0.0 0.0.0.0 area 0
- router ospf 1
  default-information originate
- router ospf 1
  redistribute static subnets
- router ospf 1
  redistribute connected 0.0.0.0

Which protocol does MPLS use to support traffic engineering?

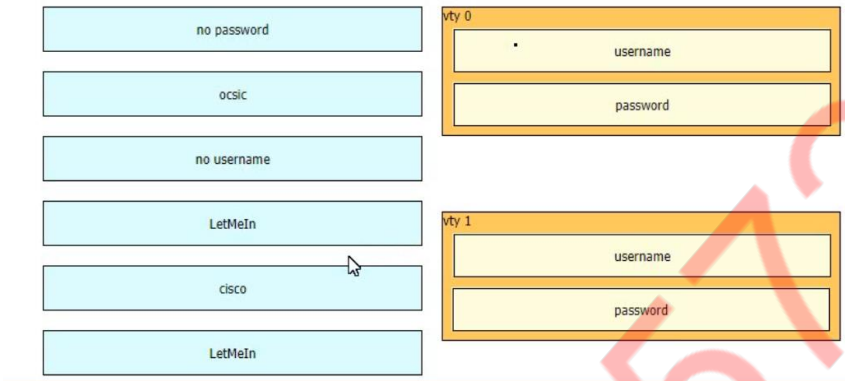
- TDP
- BGP
- LDP
- RSVP

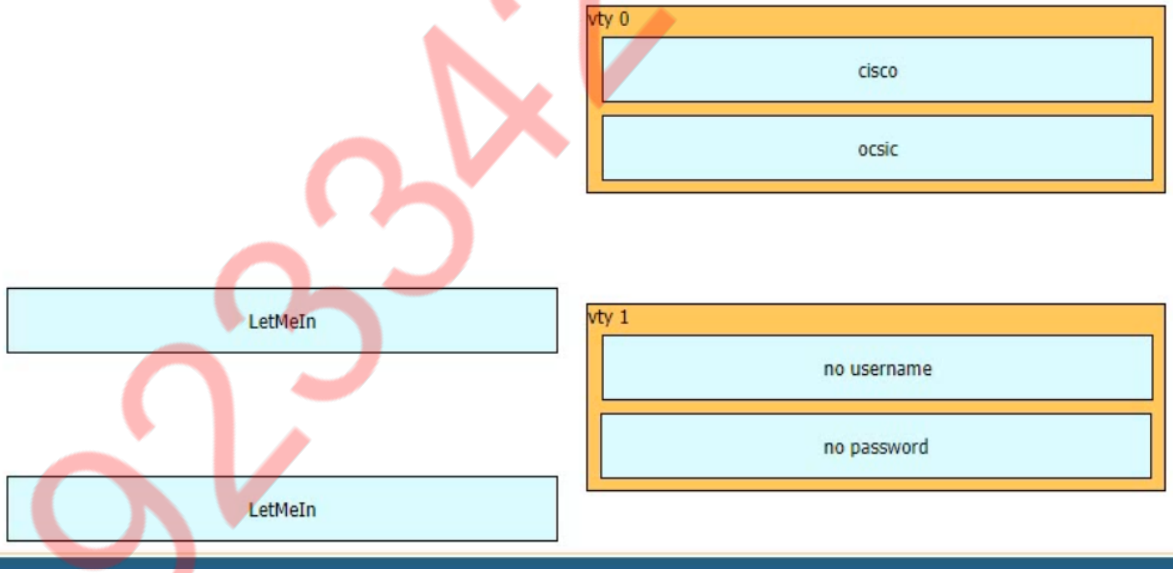
+923342572268

Taken on 7th Sep

```
line vty 0
 password LetMeIn
 login authentication telnet
 transport input telnet
line vty 1
 password LetMeIn
 transport input telnet
```

Refer to the exhibit. 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.





+923425722268

Taken on 7th Sep

```
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 E 0/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Cisco123
```

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

- [ ] NY
  router ospf 1
  area 0 authentication message-digest

- [ ] NY
  interface E 0/0
  no ip ospf message-digest-key 1 md5 Cisco123
  ip ospf authentication-key Cisco123

- [x] LA
  interface E 0/0
  ip ospf authentication-key Cisco123

- [ ] LA
  router ospf 1
  area 0 authentication message-digest

- [x] LA
  interface E 0/0
  ip ospf message-digest-key 1 md5 Cisco123

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?

- ( ) Configure the **no logging console debugging** command globally.
- ( ) Configure the **term no mon** command globally.
- (•) Configure the **logging synchronous** command.
- ( ) Configure the **logging synchronous level all** command.

+923342572268

Taken on 7th Sep

```
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 FastEthernet0/0

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 FastEthernet0/0
   passive-interface FastEthernet0/0
```

Refer to the exhibit. R1 and R2 cannot establish an EIGRP adjacency. Which action establishes EIGRP adjacency?

- Add the **passive-interface** command to the R1 configuration so that it matches the R2 configuration.
- Remove the current autonomous system number on one of the routers and change to a different value.
- Add the **no auto-summary** command to the R2 configuration so that it matches the R1 configuration.
- Remove the **passive-interface** command from the R2 configuration so that it matches the R1 configuration.

```
 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
!
```

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

- Modify the interface command to **ip flow monitor FLOW-MONITOR-1 input**.
- Modify the flow transport command **transport udp 2055** to move under flow monitor profile.
- Modify the udp port under flow exporter profile to **ip transport udp 4739**.
- Modify the flow record command **record v4_r1** to move under flow exporter profile.

+923342557268

Taken on 7th Sep

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?

- Desired Min TX Interval
- Detect Mult
- Required Min RX Interval
- Required Min Echo RX Interval

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
```

Refer to the exhibit. 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?

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

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?

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

+923342512268

Taken on 7th Sep

Drag and drop the actions from the left into the order on the right to configure a policy to avoid following packet forwarding based on the normal routing path.

Configure route map instances.	step 1
Configure set commands.	step 2
Configure fast switching for PBR.	step 3
Configure ACLs.	step 4
Configure match commands.	step 5
Configure PBR on the interface.	step 6

Configure ACLs.

Configure route map instances.

Configure match commands.

Configure set commands.

Configure PBR on the interface.

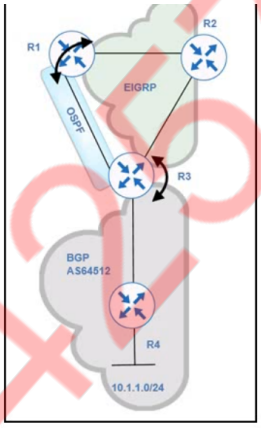
Configure fast switching for PBR.

+923342572268

Taken on 7th Sep

What are two MPLS label characteristics? (Choose two.)

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



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?

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

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

- ○ IPv4 ACL blocking route advertisements from nonauthorized hosts
- ○ VACL blocking broadcast frames from nonauthorized hosts
- ◉ PVLANs with promiscuous ports associated to route advertisements and isolated ports for nodes
- ○ PVLANs with community ports associated to route advertisements and isolated ports for nodes

+923342672268

Taken on 7th Sep

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

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

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?

- ( ) 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.
- ( ) 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.
- ( ) 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.
- (•) 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.

```
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
```

Refer to the exhibit. 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?

- ( ) Remove the prefix keyword from the **distribute-list** command.
- (•) Remove the line with the sequence number 5 from the prefix list.
- ( ) Change the direction of the **distribute-list** command from out to in.
- ( ) Remove the line with the sequence number 10 from the prefix list.

+923425572268

Taken on 7th Sep

How are MPLS Layer 3 VPN services deployed?

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

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.)

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

```
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: access-group name SNMP
        police:
            cir 8000 bps, bc 1500 bytes
          conformed 0 packets, 0 bytes; actions:
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          conformed 0000 bps, exceeded 0000 bps

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

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

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

+923342572268

Taken on 7th Sep

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

- Configure the correct authentication password using SNMPv3 authNoPriv.
- Configure the correct authentication password using SNMPv3 authPriv.
- Configure correct authentication and privacy passwords using SNMPv3 authNoPriv.
- Configure correct authentication and privacy passwords using SNMPv3 authPriv.

A customer reports to the support desk that they cannot print from their PC to the local printer id:405379016. Which tool must be used to diagnose the issue using Cisco DNA Center Assurance?

- ACL trace
- device trace
- path trace
- application trace

Filtered

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
```

Desired

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2 *Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2
```

Refer to the exhibits. An engineer filtered messages based on severity to minimize log messages. After applying the filter, the engineer noticed that it filtered required messages as well. Which action must the engineer take to resolve the issue?

- Configure syslog level 2.
- Configure syslog level 3.
- Configure syslog level 4.
- Configure syslog level 5.

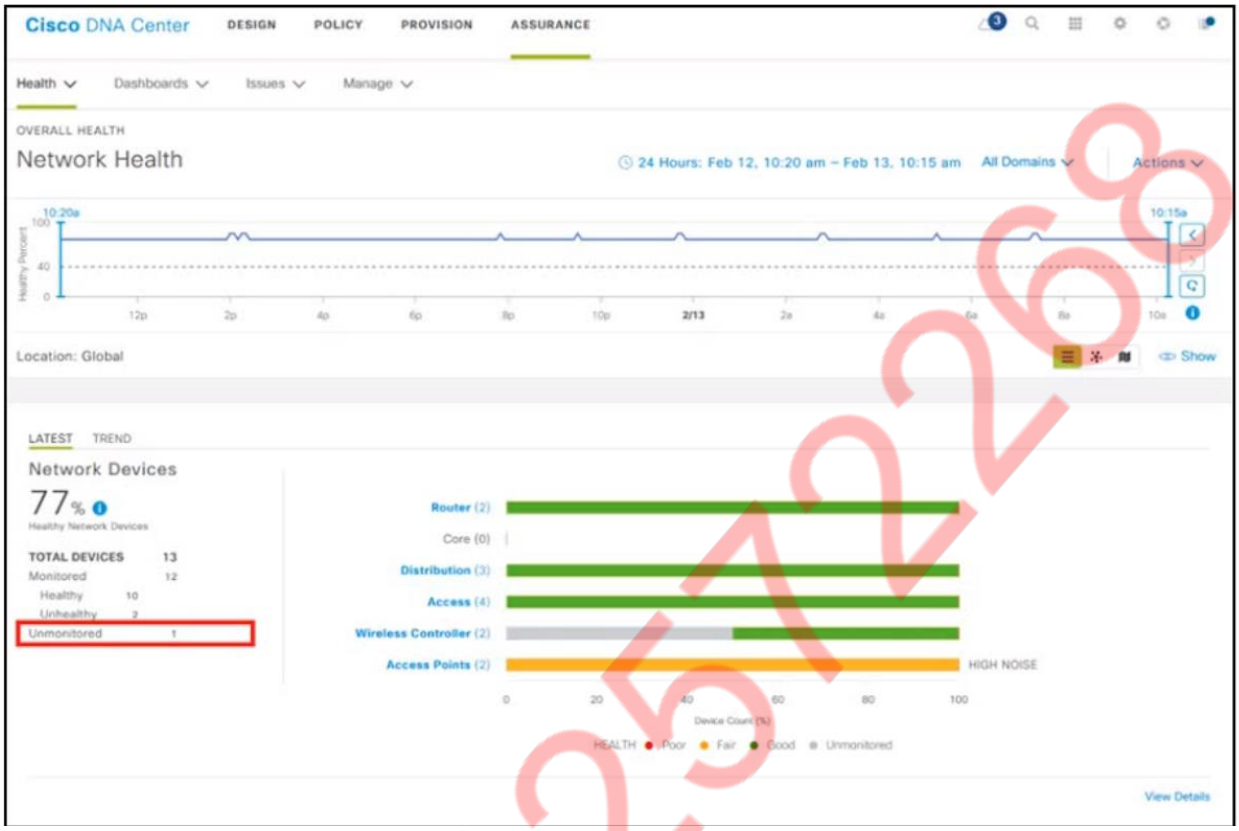
```
Spoke# show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:2,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.18.16.2 192.168.1.1 UP 01:05:35 S
1 172.18.46.2 192.168.1.4 UP 00:00:25 D
```

Refer to the exhibit. An engineer has configured DMVPN on a spoke router. What is the WAN IP address of another spoke router within the DMVPN network?

- 172.18.16.2
- 192.168.1.4
- 192.168.1.1
- 172.18.46.2

+923342172268

Taken on 7th Sep

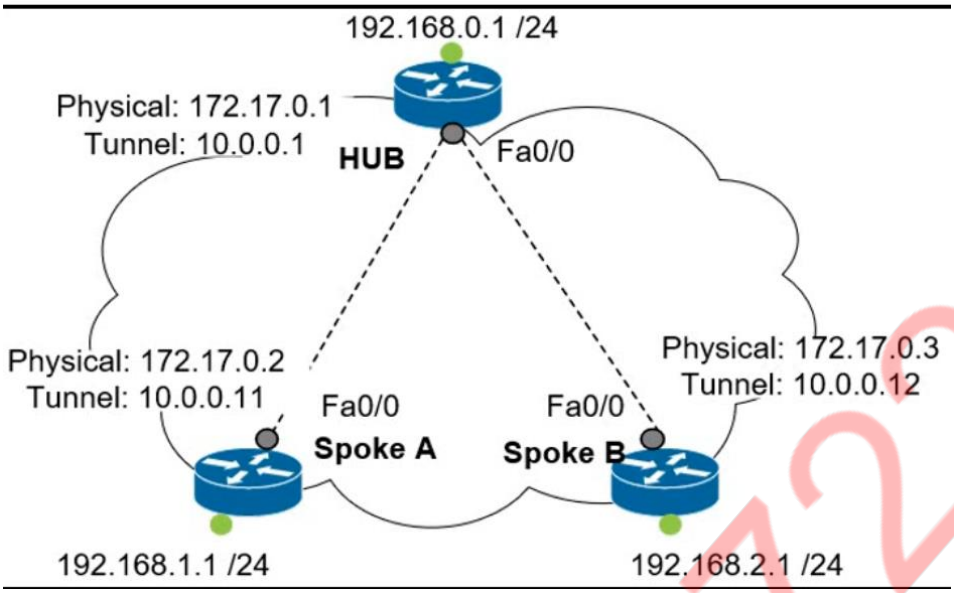


Refer to the exhibit. A network administrator added one router in the Cisco DNA Center and checked its discovery and health from the Network Health Dashboard. The network administrator observed that the router is still showing up as unmonitored. What must be configured on the router to mount it in the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

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

+923342567269

Taken on 7th Sep



Refer to the exhibit. Which interface configuration must be configured on the HUB router to enable MVPN with mGRE mode?

- 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

- 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

- (•) 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

- 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

+923425722268

Taken on 7th Sep

```
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 is 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
```

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?

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

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 17179272
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
```

Refer to the exhibit. 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?

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

+923425 1268

Taken on 7th Sep

```
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 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
```

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?

- interface Tunnel1
  tunnel protection ipsec profile IPSec-PROFILE
- interface Tunnel1
  tunnel mode ipsec ipv4
- interface Tunnel1
  no ip split-horizon eigrp 111
- interface Tunnel1
  ip next-hop-self eigrp 111

---

cisco

Congratulations, you have achieved a score of 892
A minimum of 825 is required.
Scoring is based on a scale of 300 to 1000 points.

A preliminary score report summarizing your results will be provided to you as you leave the testing center. The score information displayed on this report is preliminary and does not constitute an official score report.

Cisco seeks to assure the validity of exam score by analyzing exam responses for consistency. Your score may be classified as indeterminate if Cisco cannot certify that it represents a valid measure of your ability as sampled by the exam. After review and analysis, your scores will either be:

a) Classified as "valid" and your final result will be posted online at www.pearsonvue.com/authenticate within 72 hours of your exam session; or

b) Classified as indeterminate and you will be advised of the options for retaking the examination.

Our primary method of communication is e-mail. Please verify that you have provided a correct e-mail address during exam registration to ensure that you receive important program updates and announcements. Refer to your preliminary score report for instructions regarding verifying and updating your personal information in the Cisco Career Certifications Tracking System.

Cisco policy requires that you wait a minimum of 180 days before retaking a passed exam (with an identical exam number).

+923425772268