

➤ **Vendor: Cisco**

➤ **Exam Code: 300-410**

➤ **Exam Name: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [March/2021](#))**

[Visit Braindump2go and Download Full Version 300-410 Exam Dumps](#)

QUESTION 147

How are MPLS Layer 3 VPN services deployed?

- A. The RD and RT values must match under the VRR
- 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.

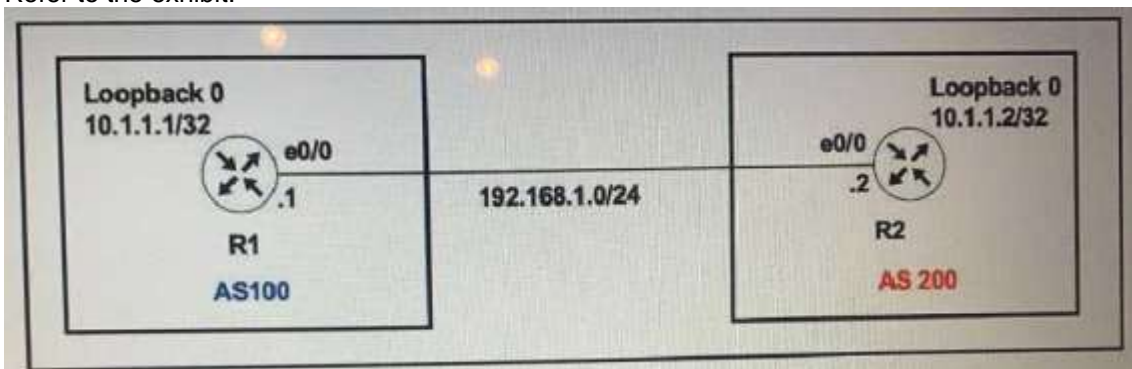
Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/vpn/65x/b-l3vpn-cg-ncs5500-65x/b-l3vpn-cg-ncs5500-65x_chapter_010.html

QUESTION 148

Refer to the exhibit.



The R1 and R2 configurations are:

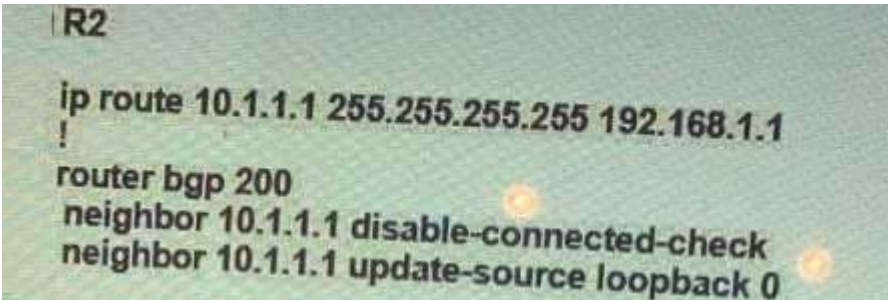
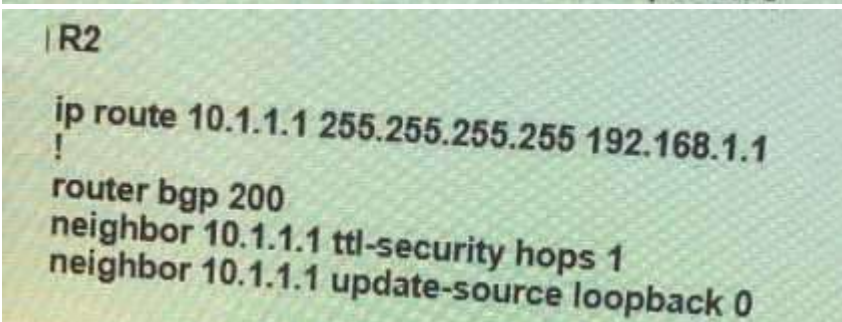
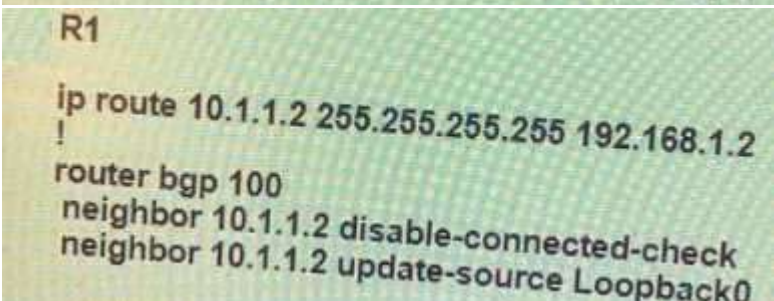
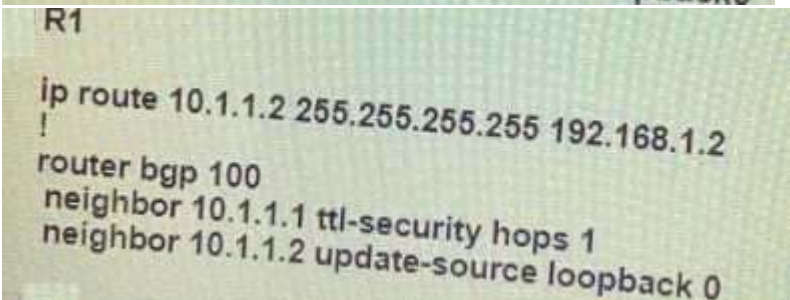
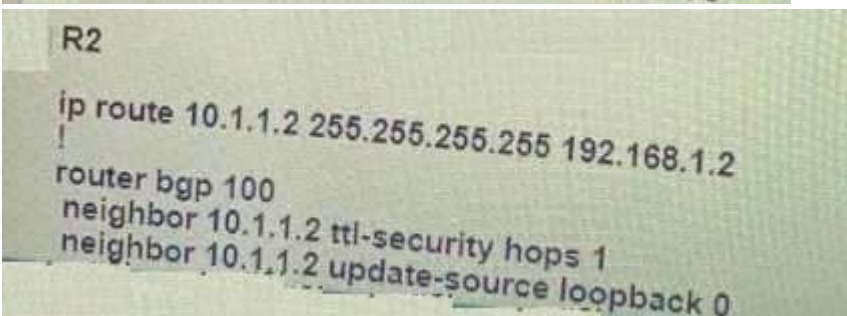
```
R1
router bgp 100
neighbor 10.1.1.2 remote-as 200

R2
router bgp 200
neighbor 10.1.1.1 remote-as 100
```

The neighbor is not coming up. Which two sets of configurations bring the neighbors up? (Choose two.)

[300-410 Exam Dumps](#) [300-410 Exam Questions](#) [300-410 PDF Dumps](#) [300-410 VCE Dumps](#)

<https://www.braindump2go.com/300-410.html>

- A. 
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 loopback 0
- B. 
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
- C. 
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
- D. 
R1
ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
neighbor 10.1.1.1 ttl-security hops 1
neighbor 10.1.1.2 update-source loopback 0
- E. 
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

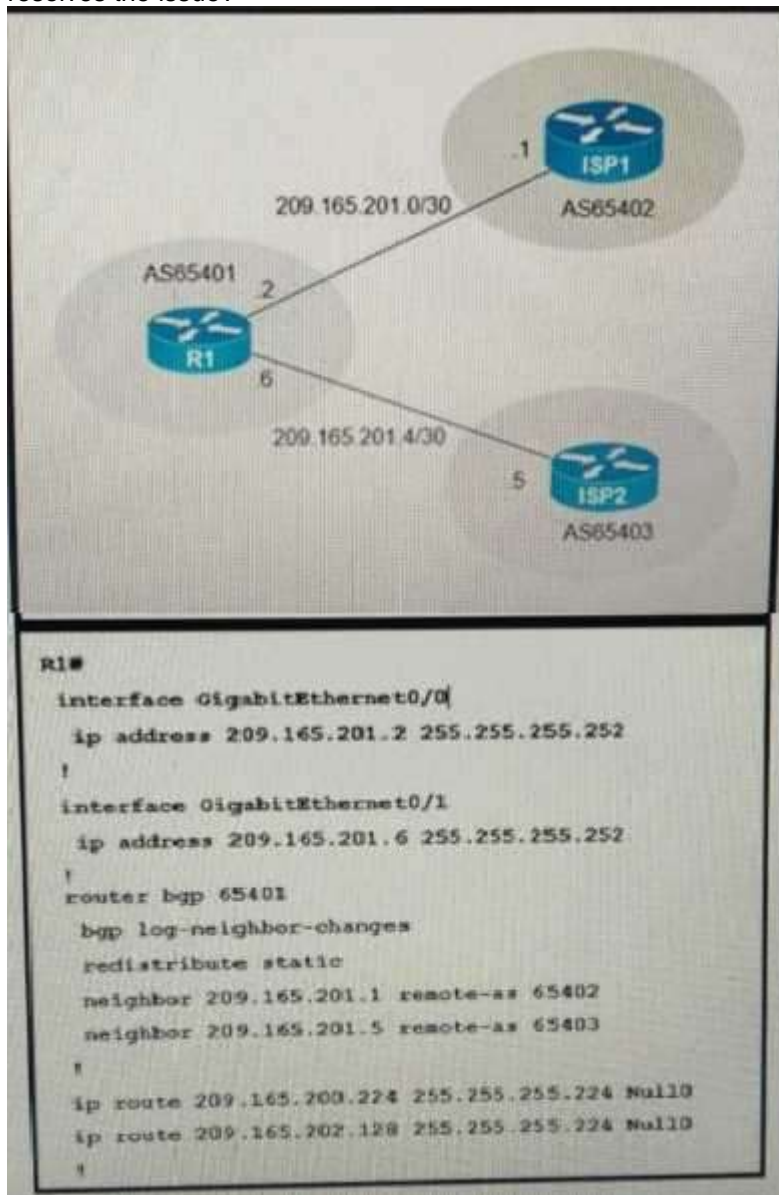
Answer: AC

Explanation:

The `neighbor disable-connected-check` command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

QUESTION 149

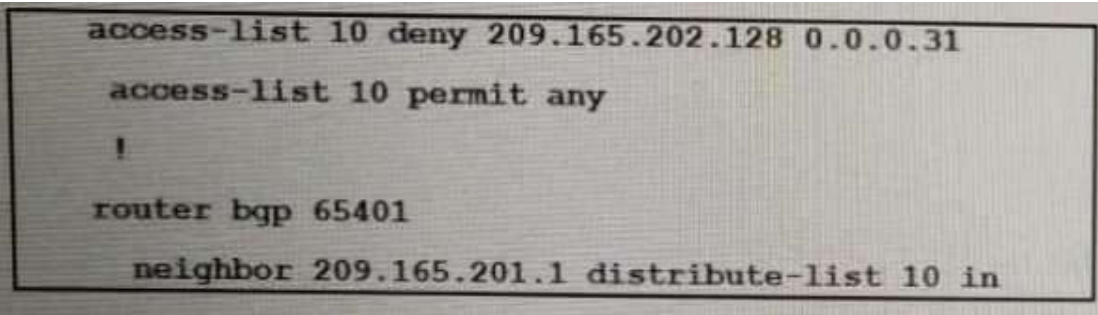
Refer to the exhibit. A company with autonomous system number AS6 401 has obtained IP address block 209.165.200.224/27 from ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer is ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration on R1 resolves the issue?

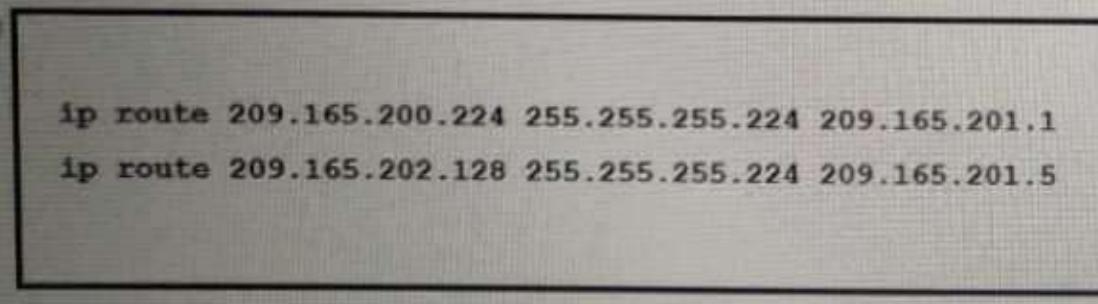


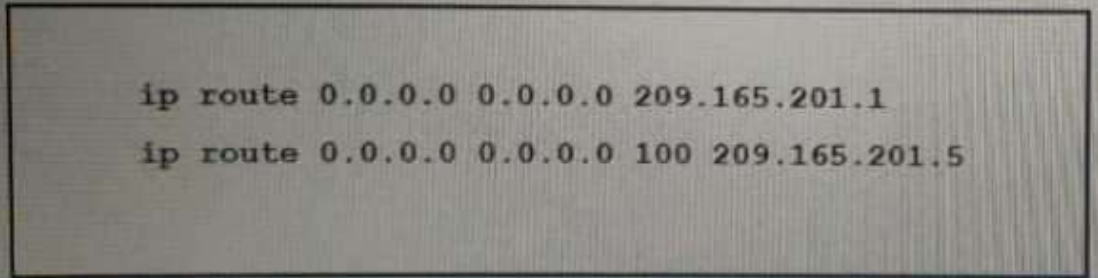
A.

```

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 0.0.0.0 100 209.165.201.5
```

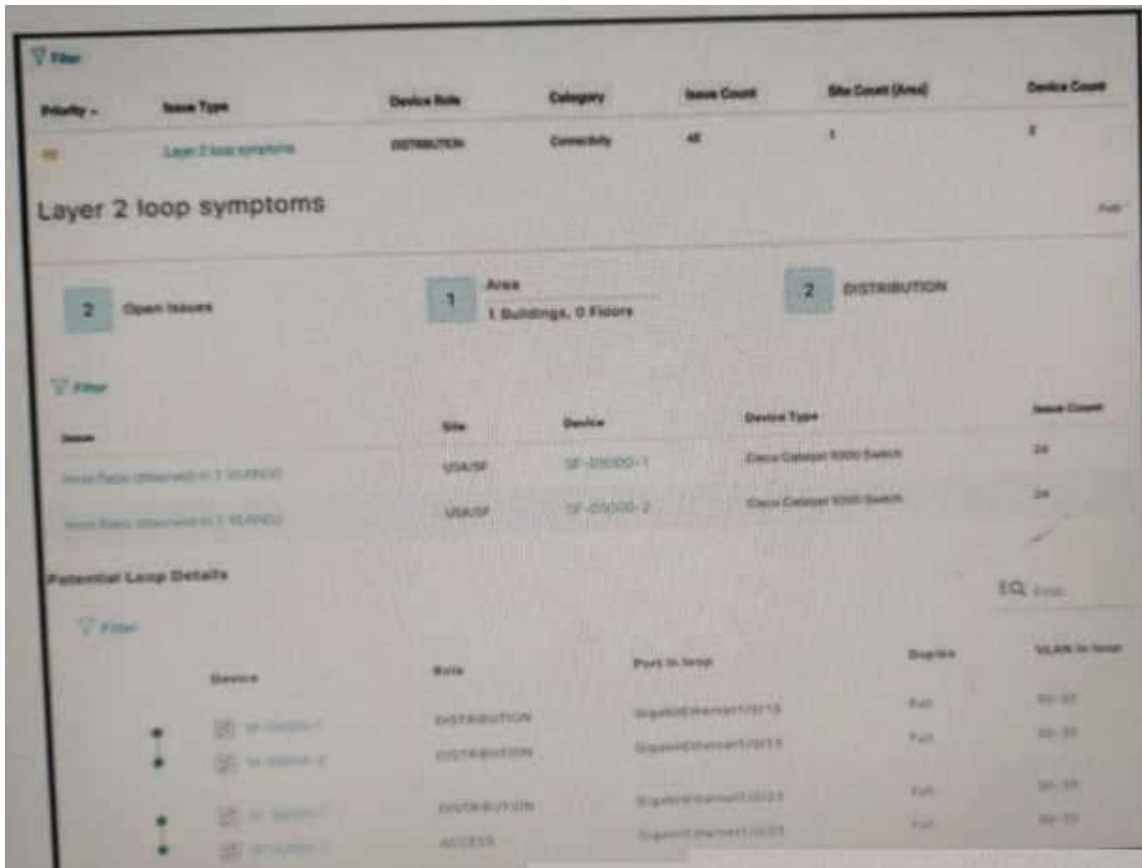
Answer: A

Explanation:

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html>

QUESTION 150

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



The screenshot shows the Cisco DNA Center interface for troubleshooting Layer 2 loop symptoms. It includes a summary section with filters for Open Issues (2), Area (1 Building, 0 Floors), and Distribution (2). Below this is a table of issues and a detailed view of potential loop details.

Issue	Site	Device	Device Type	Issue Count
Issue 1: Loop observed in 1 VLAN	USA/SP	SP-21000-1	Dense Catalyst 9500 Switch	24
Issue 2: Loop observed in 1 VLAN	USA/SP	SP-21000-2	Dense Catalyst 9500 Switch	24

Device	Role	Port in Loop	Duplex	VLAN in Loop
SP-21000-1	DISTRIBUTION	GigabitEthernet1/0/13	Full	30-33
SP-21000-2	DISTRIBUTION	GigabitEthernet1/0/13	Full	30-33
SP-21000-1	DISTRIBUTION	GigabitEthernet1/0/23	Full	30-33
SP-21000-2	ACCESS	GigabitEthernet1/0/23	Full	30-33

```
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
```

- A. no spanning-tree uplinkfast
- B. spanning-tree loopguard default
- C. spanning-tree backbonesfast
- D. spanning-tree portfast bpduguard

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/b_dnac_sda_lan_automation_deployment.html

QUESTION 151

What are two functions of LDP? (Choose two.)

- A. It is defined in RFC 3038 and 3039.
- B. It requires MPLS Traffic Engineering.
- C. It advertises labels per Forwarding Equivalence Class.

[300-410 Exam Dumps](#) [300-410 Exam Questions](#) [300-410 PDF Dumps](#) [300-410 VCE Dumps](#)

<https://www.braindump2go.com/300-410.html>

- D. It must use Resource Reservation Protocol.
- E. It uses Forwarding Equivalence Class

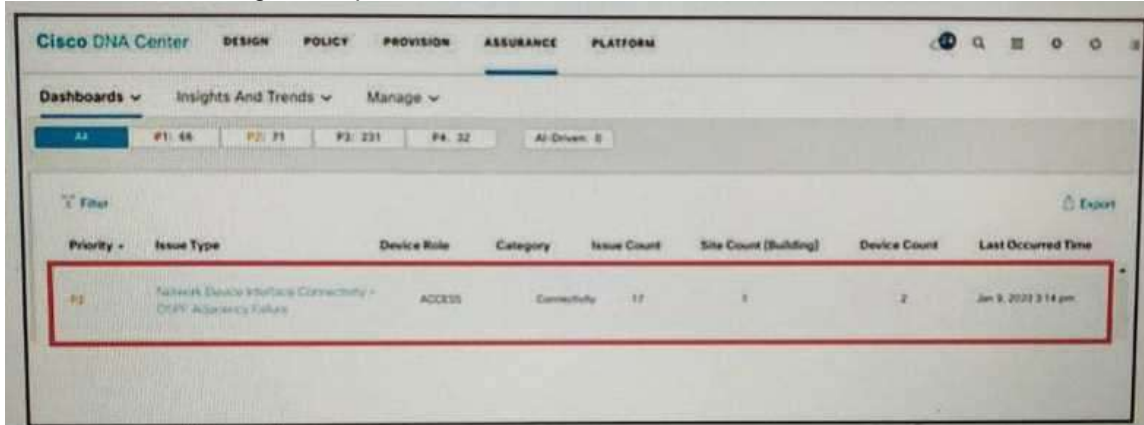
Answer: CE

Explanation:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/mppls/configuration/guide/mppls_cg/mp_mpls_overview.pdf

QUESTION 152

Refer to the exhibit. 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 neighborhood is stuck in exstart state. How does the administrator fix this issue?



Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Building)	Device Count	Last Occurred Time
P2	Network Device Interface Connectivity - OSPF Adjacency Failure	ACCESS	Connectivity	17	1	2	Jan 9, 2020 3:14 pm

- A. Configure to match the OSPF interface speed and duplex settings on both routers.
- B. Configure to match the OSPF interface MTU settings on both routers.
- C. Configure to match the OSPF interface unique IP address and subnet mask on both routers.
- D. Configure to match the OSPF interface network types on both routers.

Answer: B

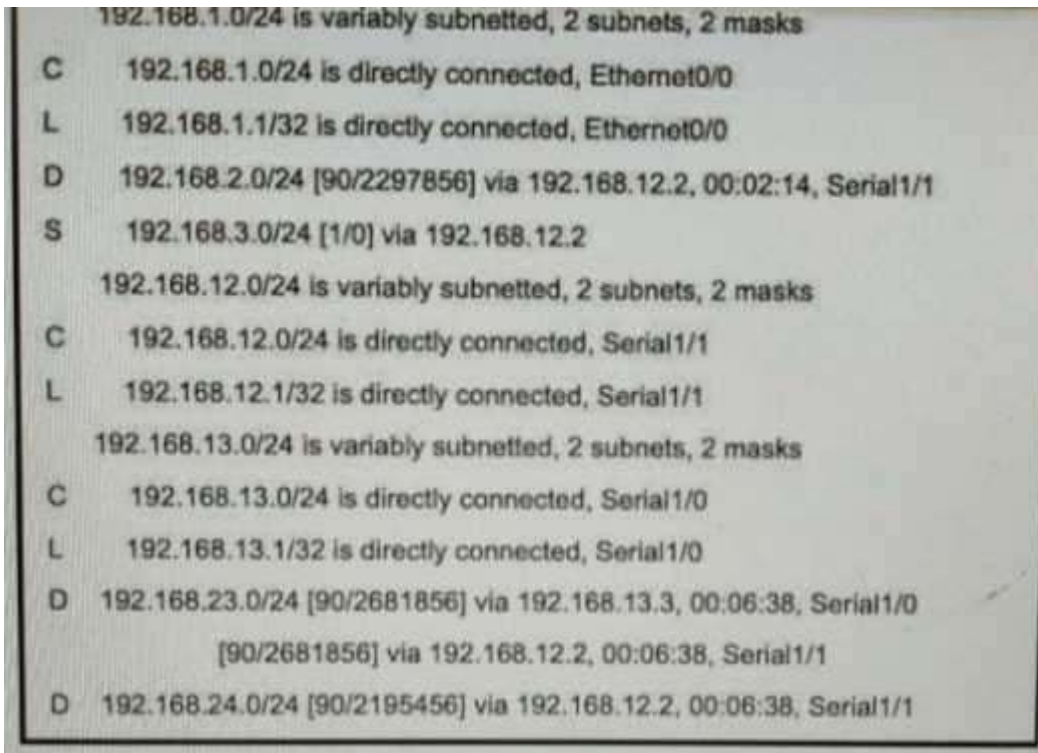
Explanation:

After two OSPF neighboring routers establish bi-directional communication and complete DR/BDR election (on multi-access networks), the routers transition to the exstart state. In this state, the neighboring routers establish a master/slave relationship and determine the initial database descriptor (DBD) sequence number to use while exchanging DBD packets. Neighbors Stuck in Exstart/Exchange State The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13684-12.html>

QUESTION 153

Refer to the exhibit. All the serial between R1, R2, and R3 have the Same bandwidth. 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 154

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?

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

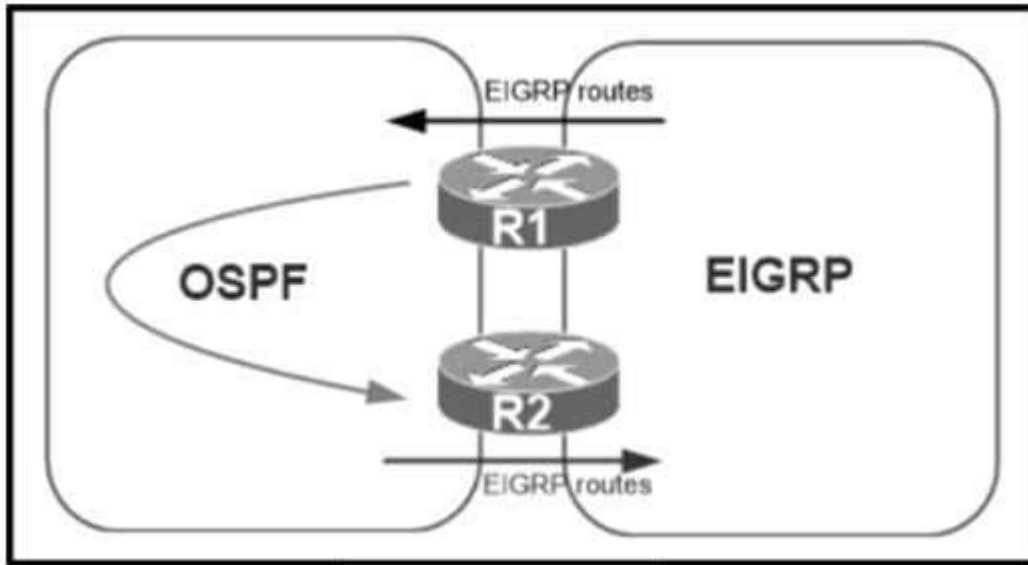
Answer: A

Explanation:

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when this device receives traps. "Send reliable and encrypted notifications for any events" so it is SNMP notifications. For encryption we need to configure "priv".

QUESTION 155

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. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.
- C. 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.
- D. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.

Answer: C

Explanation:

When doing mutual redistribution at multiple points (between OSPF and EIGRP on R1 & R2), we may create routing loops so we should use route-map to prevent redistributed routes from redistributing again into the original domain. In the below example, the route-map "SET-TAG" is used to prevent any routes that have been redistributed into EIGRP from redistributed again into OSPF domain by tagging these routes with tag

1:

```
R3
route-map SET-TAG permit 10
set tag 1
```

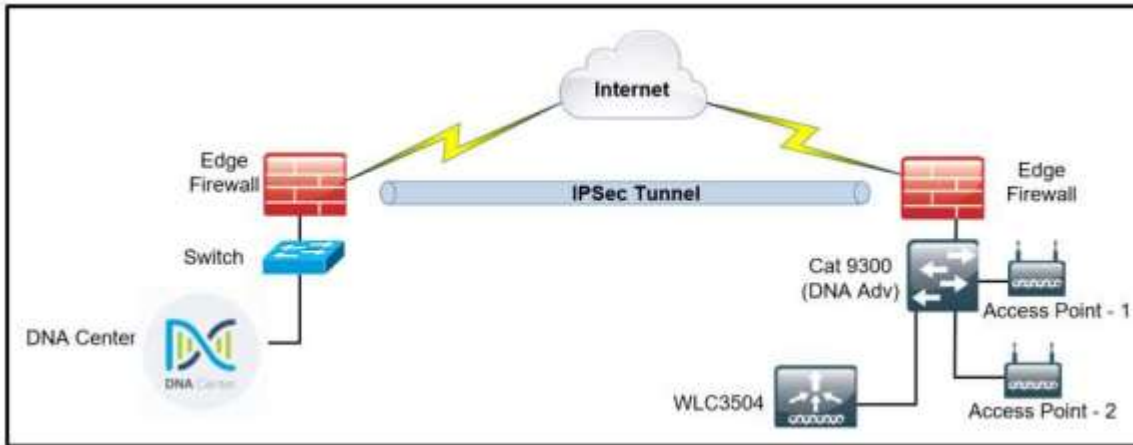
These routes are prevented from redistributed again by route-map FILTER_TAG by denying any routes with tag 1 set:

```
R4
route-map FILTER-TAG deny 10
match tag 1
```

QUESTION 156

Refer to the exhibit. A network administrator is discovering a Cisco Catalyst 9300 and a Cisco WLC 3504 in Cisco DNA Center. The Catalyst 9300 is added successfully However the WLC is showing [error "uncontactable" when the administrator tries to add it in Cisco DNA Center.

Which action discovers WLC in Cisco DNA Center successfully?



- A. Copy the .cert file from the 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 .pern file from the Cisco DNA Center on the USB and upload it to the WLC 3504.

Answer: D

QUESTION 157

Which feature drops packets if the source address is not found in the snooping table?

- A. IPv6 Source Guard
- B. IPv6 Destination Guard
- C. IPv6 Prefix Guard
- D. Binding Table Recovery

Answer: A

QUESTION 158

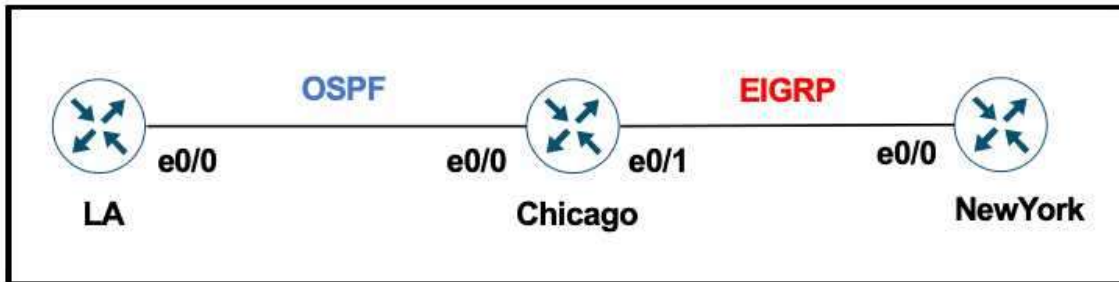
Refer to the exhibit. A user has set up an IP SLA probe to test if a non SLA host web server on IP address 10.1.1.1 accepts HTTP sessions prior to deployment. The probe is failing. Which action should the network administrator recommend for the probe to succeed?



The diagram shows four routers (R1, R2, R3, R4) and their connections. R1, R2, and R3 are in a single AS, while R4 is in a separate AS. R1 and R2 are connected via a BGP link (10.10.10.0/24, Metric 10). R1 and R3 are connected via a BGP link (10.10.20.0/24, Metric 1). R2 and R3 are connected via an OSPF link (10.10.30.0/24, Metric 1). R4 is connected to R3 via a BGP link (10.11.11.0/24, Metric 1). R4's interfaces are 10.1.1.0/24 and 10.1.2.0/24.

- Answer: A**

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 metric 20
```
- B.

```
router eigrp 100
 redistribute ospf 1 metric 10 10 10 10 10
```
- C.

```
router eigrp 100
 redistribute ospf 1 subnets
```
- D.

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

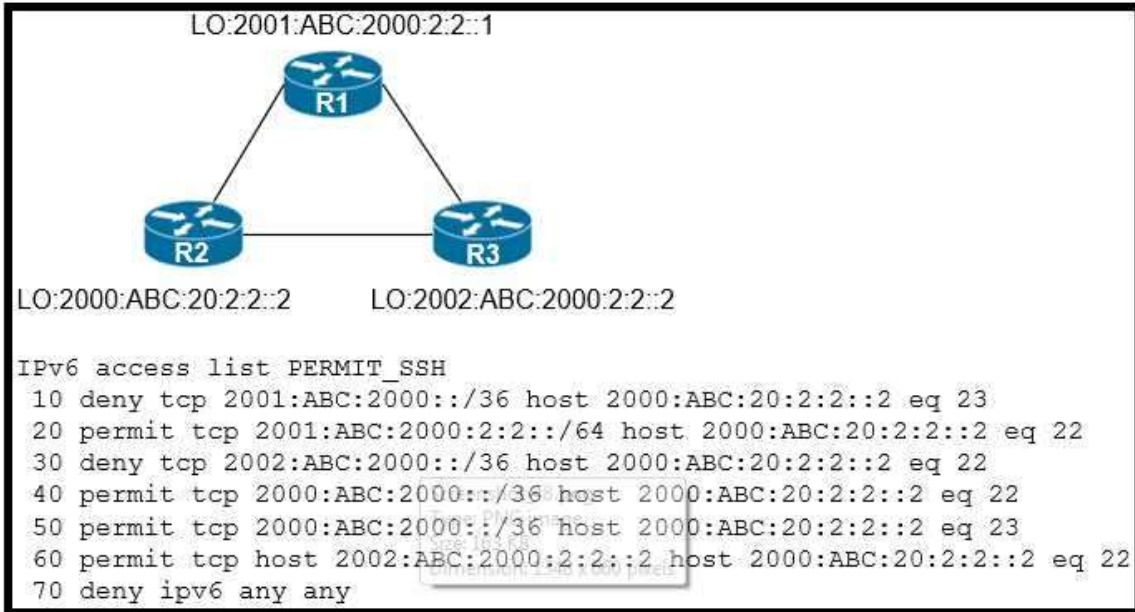
Answer: B

Explanation:

"LA router receives all the NewYork routes but it does not receive any LA routes" because when redistributing into EIGRP, we must configure the default metric.

QUESTION 160

Refer to the exhibit. 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 161

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?

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

Answer: A

Explanation:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.pdf>

There are three SNMP security levels (for SNMPv1, SNMPv2c, and SNMPv3):

+ noAuthNoPriv: Security level that does not provide authentication or encryption.

+ authNoPriv: Security level that provides authentication but does not provide encryption.

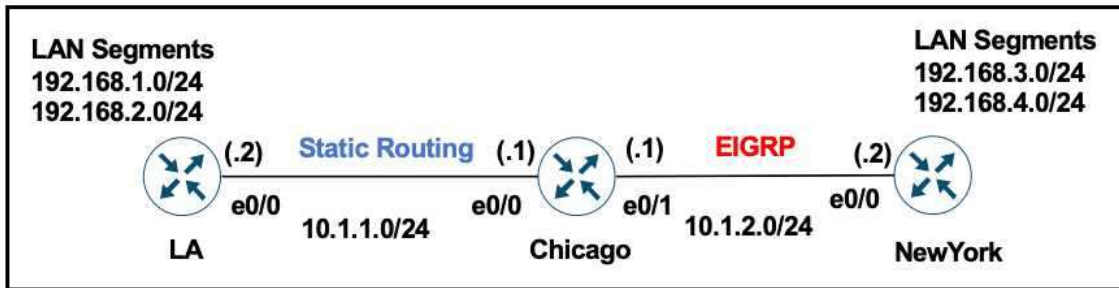
+ authPriv: Security level that provides both authentication and encryption.

For SNMPv3, "noAuthNoPriv" level uses a username match for authentication.

QUESTION 162

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?



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

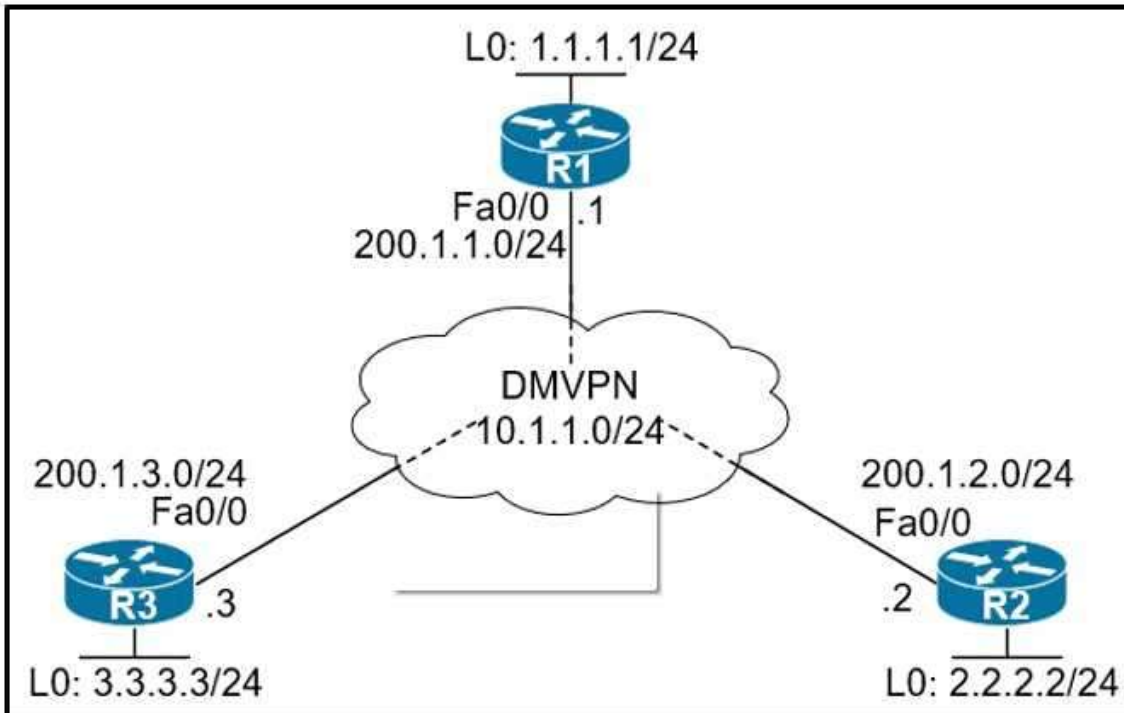
```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

- A. Chicago Router
- ```
router eigrp 100
 redistribute static metric 10 10 10 10 10
```
- B. Chicago Router
- ```
router eigrp 100
 redistribute connected
```
- C. 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
```
- D. 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
```

Answer: A

QUESTION 163

Refer to the exhibits. When DMVPN is configured, which configuration allows spoke-to-spoke communication using loopback as tunnel source?



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
```

- 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: A

QUESTION 164

What are two functions of IPv6 Source Guard? (Choose two.)

- A. It uses the populated binding table for allowing legitimate traffic.
- B. It works independent from IPv6 neighbor discovery.
- C. It denies traffic from unknown sources or unallocated addresses.
- D. It denies traffic by inspecting neighbor discovery packets for specific pattern.
- E. It blocks certain traffic by inspecting DHCP packets for specific sources.

[300-410 Exam Dumps](#) [300-410 Exam Questions](#) [300-410 PDF Dumps](#) [300-410 VCE Dumps](#)

<https://www.braindump2go.com/300-410.html>

Answer: AC

QUESTION 165

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: 388213827 packets, 222009685077 bytes
```

What are the two effects of this route map configuration? (Choose two.)

- A. Packets are not evaluated by sequence 10.
- B. Packets are evaluated by sequence 10.
- C. Packets are forwarded to the default gateway.
- D. Packets are forwarded using normal route lookup.
- E. Packets are dropped by the access list.

Answer: BC

QUESTION 166

Refer to the exhibit. Which two actions restrict access to router R1 by SSH? (Choose two.)

```
R1#show policy-map control-plane
Control Plane
Service-policy 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 0000 bps
    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 list 199
  10 deny tcp any eq telnet any (50 matches)
  50 permit ip any any (1 match)

R1#show running-config | section line vty
line vty 0 4
login
transport input telnet ssh
transport output telnet ssh
```

- 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 20 from access list 100.
- C. Remove class-map ANY from service-policy CoPP
- D. Configure transport output ssh on line vty and remove sequence 10 from access list 199.
- E. Remove sequence 10 from access list 100 and add sequence 20 deny tcp any any eq telnet to access list 199

Answer: AB

Explanation:

To only allow SSH to R1, we have to: + Deny Telnet in ACL 100 because the action of class-map: PERMIT is "permit" + Permit Telnet in ACL 199 because the action of class-map: ANY is "drop" But: + In ACL 100 there is a permit statement for Telnet traffic "20 permit tcp any any eq telnet (5 matches)" which is not correct so we must remove this statement.
+ In ACL 199 there is an ACL statement "10 deny tcp any eq telnet any (50 matches)". This statement is aimed for Telnet traffic leaving R1 which is not correct so we must remove this statement.

Note:

+ The command "transport output telnet ssh" allows telnet and SSH from this device (to other devices).

[300-410 Exam Dumps](#) [300-410 Exam Questions](#) [300-410 PDF Dumps](#) [300-410 VCE Dumps](#)

<https://www.braindump2go.com/300-410.html>

+ Telnet is TCP port 23. + When using Telnet on source port, it affects Telnet traffic leaving from R1.

QUESTION 167

Refer to the exhibit. 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?

```
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
```

- A. Configure logging history 2
- B. Configure logging history 3
- C. Configure logging history 4
- D. Configure logging history 5

Answer: D

Explanation:

By default, the maximum severity sent as a syslog trap is warning. That is why you see syslog traps for login failures. Since a login success is severity 5 (notifications), those syslog messages will not be converted to traps. To fix this, configure:

logging history 5

Syslog levels are listed below

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Note:

The syntax of login block is:

login block-for seconds attempts tries within seconds

QUESTION 168

Drag and Drop Question

Drag and drop the actions from the left into the correct 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

Answer:

	Configure ACLs.
	Configure route map instances.
	Configure match commands.
	Configure set commands.
	Configure PBR on the interface.
	Configure fast switching for PBR.

Explanation:

<https://community.cisco.com/t5/networking-documents/how-to-configure-pbr/ta-p/3122774>