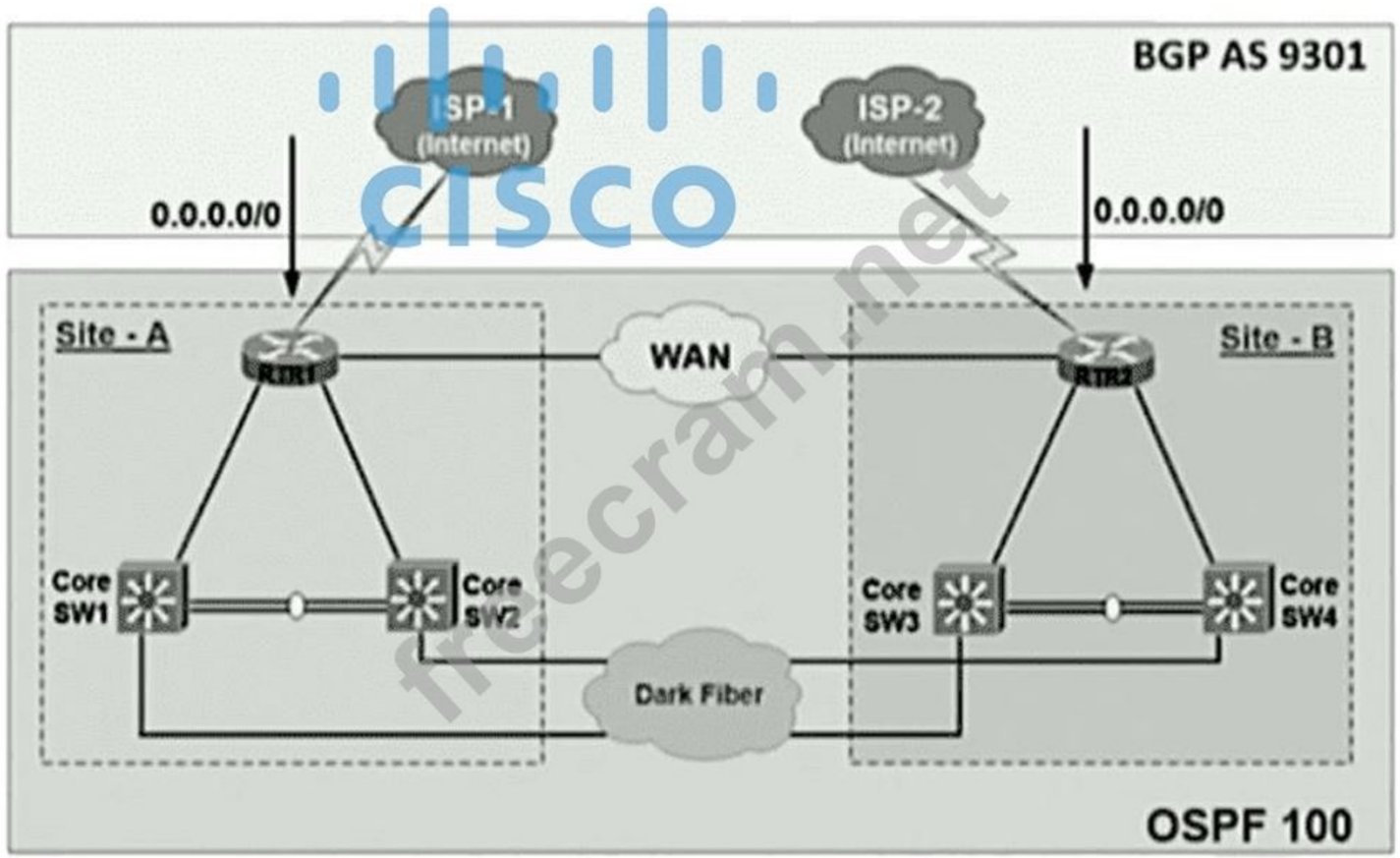
Cisco.300-410.v2026-06-19.q279

Exam Code:	300-410
Exam Name:	Implementing Cisco Enterprise Advanced Routing and Services
Certification Provider:	Cisco
Free Question Number:	279
Version:	v2026-06-19
# of views:	102
# of Questions views:	2800
https://www.freecram.net/torrent/Cisco.300-410.v2026-06-19.q279.html	

NEW QUESTION: 1
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 metric-type 2 at Site-A RTR1, and set metric-type 1 at Site-B RTR2

B. Set OSPF cost 100 at Site-A RTR1, and set OSPF Cost 200 at Site-B RTR2

C. Set OSPF cost 200 at Site: A RTR1 and set OSPF Cost 100 at Site-B RTR2

D. Set metric-type 1 at Site-A RTR1, and set metric-type 2 at Site-B RTR2

Answer: (SHOW ANSWER)

OSPF type 1 route is always preferred over a type 2 route for the same destination so we can set metric-type 1 at Site-A RTR1 so that it is preferred over Site-B RTR2.

Note:

Routes are redistributed in OSPF as either type 1 (E1) routes or type 2 (E2) routes, with type 2 being the default.

- A type 1 route has a metric that is the sum of the internal OSPF cost and the external redistributed cost.
- A type 2 route has a metric equal only to the redistributed cost.
- If routes are redistributed into OSPF as type 2 then every router in the OSPF domain will see the same cost to reach the external networks.
- If routes are redistributed into OSPF as type 1, then the cost to reach the external networks could vary from router to router.

NEW QUESTION: 2

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: (SHOW ANSWER)

The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link, and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.The feature enables the filtering of IPv6 traffic based on the destination address, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknown destination.

Reference: https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/IPv6_Security.pdf

NEW QUESTION: 3

Which transport layer protocol is used to form LDP sessions?

A. UDP

B. SCTP

C. TCP

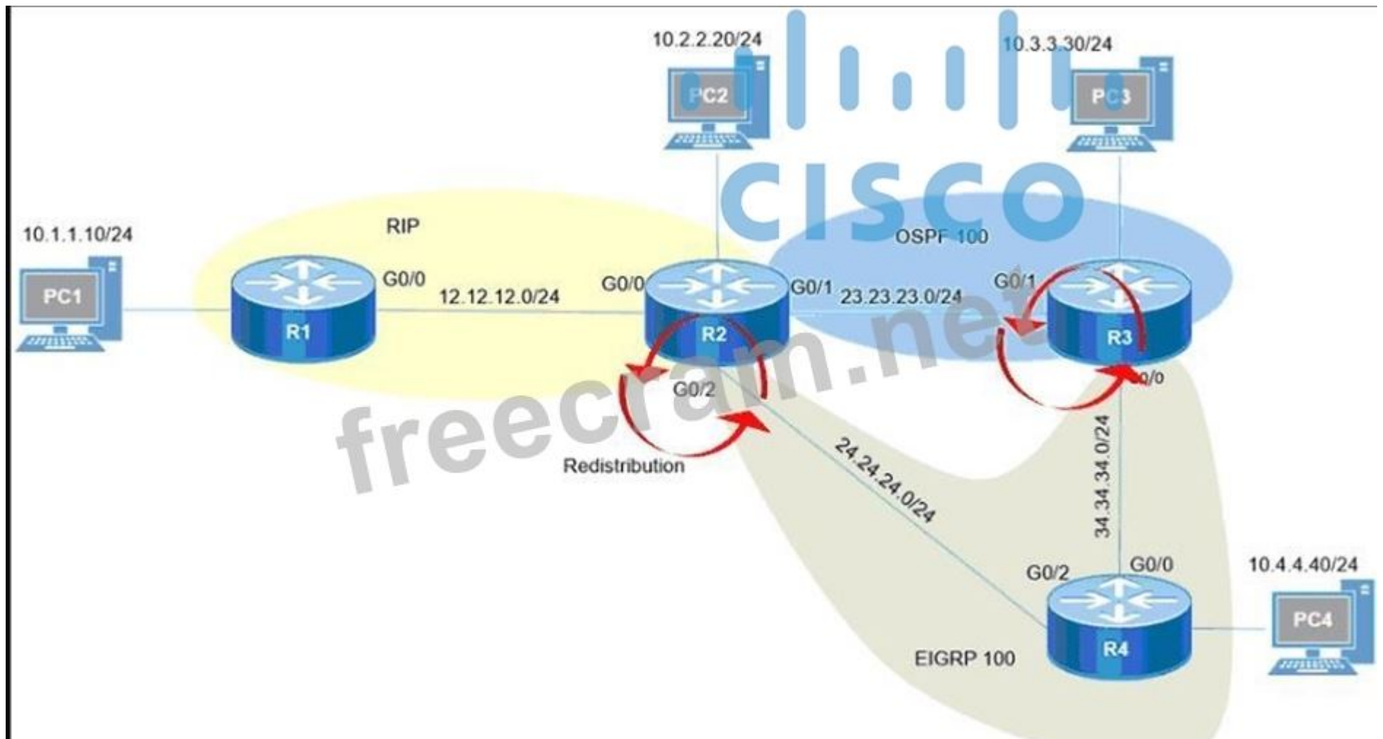
D. RDP

Answer: (SHOW ANSWER)

LDP multicasts hello messages to a well-known UDP port (646) in order to discover neighbors. Once the discovery is accomplished, a TCP connection (port 646) is established and the LDP session begins. LDP keepalives ensure the health of the session. Thanks to the LDP session, LDP messages create the label mappings required for a FEC. Withdraw messages are used when FECs need to be torn down.

NEW QUESTION: 4

Refer to the exhibit.



Redistribution is enabled between the routing protocols, and nowPC2 PC3, and PC4 cannot reach PC1. What are the two solutions to fix the problem? (Choose two.)

A. Filter RIP routes back into RIP when redistributing into RIP in R2

B. Filter OSPF routes into RIP FROM EIGRP when redistributing into RIP in R2.

C. Filter all routes except RIP routes when redistributing into EIGRP in R2.

D. Filter RIP AND OSPF routes back into OSPF from EIGRP when redistributing into OSPF in R2

E. Filter all routes except EIGRP routes when redistributing into OSPF in R3.

Answer: A,C (LEAVE A REPLY)

Even PC2 cannot reach PC1 so there is something wrong with RIP redistribution in R2. Because RIP has higher Administrative Distance (AD) value than OSPF and EIGRP so it will be looped when doing mutual redistribution.

NEW QUESTION: 5

What is considered the primary advantage of running BFD?

A. reduction in time needed to detect Layer 2 switched neighbor failures

B. reduction in CPU needed to detect Layer 3 routing neighbor failures

C. reduction in CPU needed to detect Layer 2 switch neighbor failures

D. reduction in time needed to detect Layer 3 routing neighbor failures

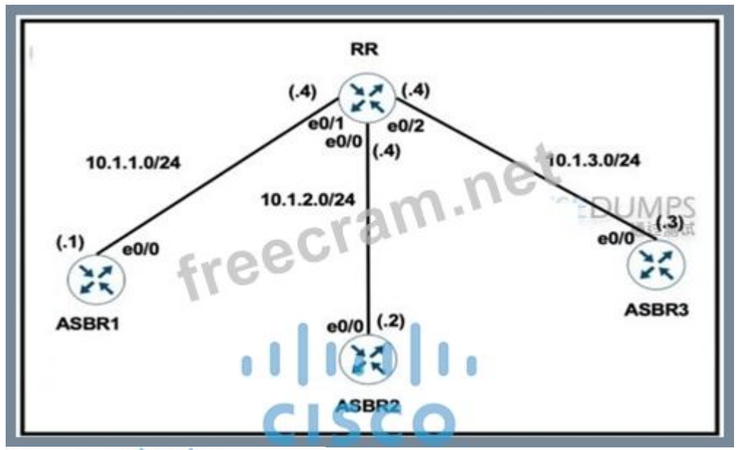
Answer: (SHOW ANSWER)

NEW QUESTION: 6

Which option is the best for protecting CPU utilization on a device?

A. COPP
B. ICMP redirects
C. ICMP unreachable messages
D. fragmentation
Answer: (SHOW ANSWER)

NEW QUESTION: 7
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. Option D
B. Option A
C. Option C
D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 8
How is the LDP router ID used in an MPLS network?
A. The MPLS LOP router ID must match the IGP router ID.
B. The loopback with the highest IP address is selected as the router ID
C. The force keyword changes the router ID to the speeded address without causing any impact.
D. If not configured, the operational physical interface is chosen as the router ID oven d a loopback is configured.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Refer to the exhibit.

```
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
```

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?
A. Configure the DHCP lease time to a smaller value
B. Configure the DHCP lease time to a bigger value
C. Modify the subnet mask to the network 192.168.1.0 255.255.254.0 command in the DHCP pool
D. Add the network 192.168.2.0 255.255.255.0 command to the DHCP pool
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
Refer to the exhibit.

```
router# show running-config
Building configuration...
!
<output omitted -----!>
!
hostname R1
!
ip domain-name cisco.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-class 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

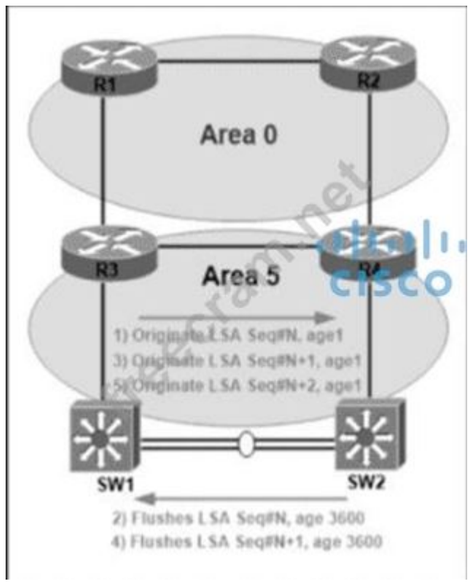
D. Configure ip ssh source-interface loopback0

Answer: A (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01001.html

NEW QUESTION: 11

Refer to the exhibit.



An error message "an OSPF-4-FLOOD_WAR" is received on SW2 from SW1. SW2 is repeatedly receiving its own link-state advertisement and flushes it from the network. Which action resolves the issue?

A. Configure Layer 3 port channel on interfaces between switches

B. Change area 5 to a normal area from a nonstub area

C. Resolve different subnet mask issue on the link

D. Resolve duplicate IP address issue in the network

Answer: (SHOW ANSWER)

NEW QUESTION: 12

What are two features of BFD? (Choose two.)

A. scalable

B. intensive on CPU for Layer 2 links

C. replaces hello messages

D. reliable

E. requires routing protocols

Answer: (SHOW ANSWER)

NEW QUESTION: 13

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

A. An interface must be associated to one VRF

B. Each VRF has a different set of routing and CEF tables.

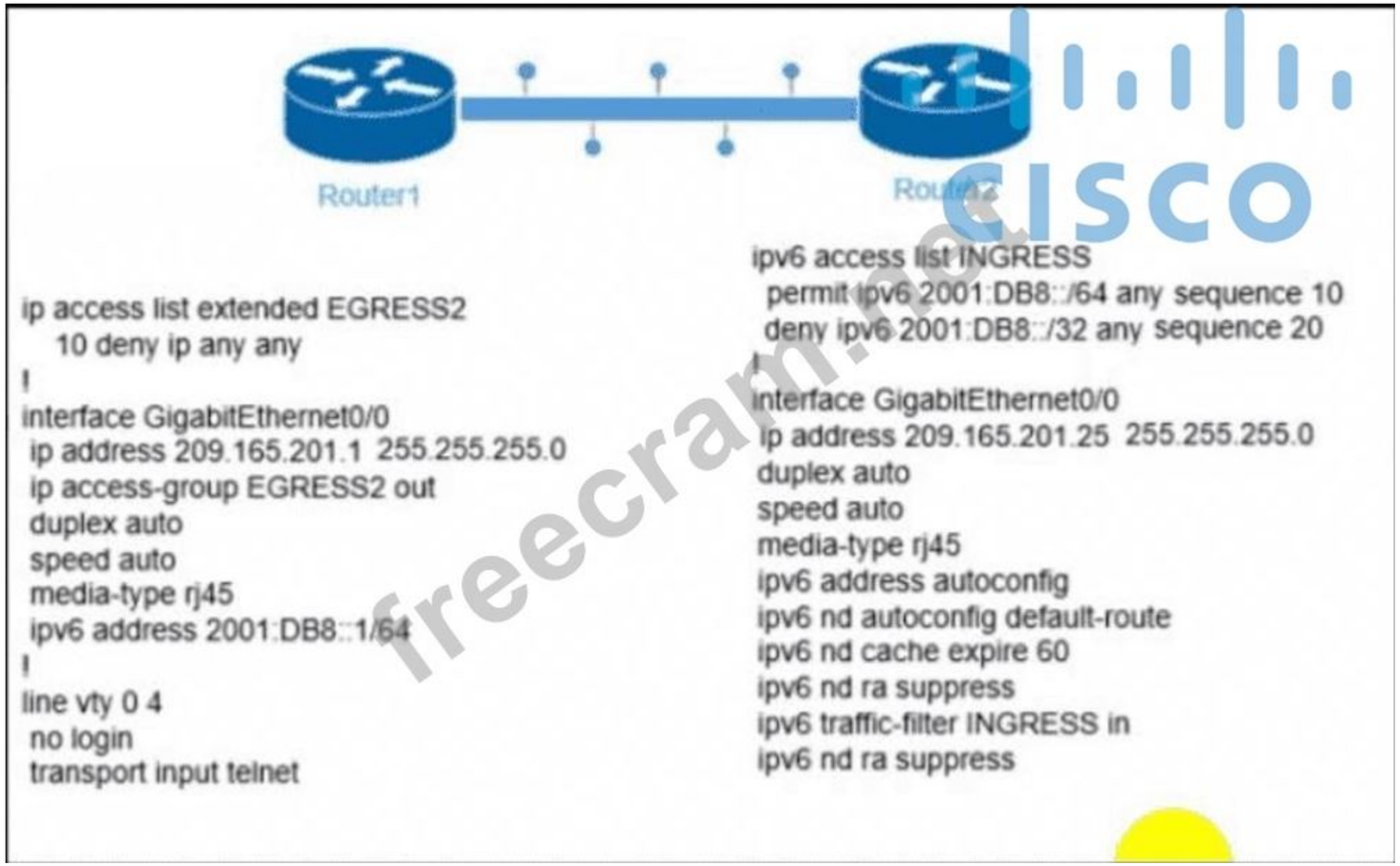
C. AII VRFS share customers routing and CEF tables.

D. It is defined by the VPN membership of a customer site attached to a P device.

E. A customer site can be associated to different VRFs.

Answer: (SHOW ANSWER)

NEW QUESTION: 14



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. jpv6 unicast-routing

B. permit ICMPv6 on access list INGRESS for Router2 to obtain IPv6 address

C. permit ip any any on access list EGRESS2 on Router1

D. IPv6 address on GigabitEthernet0/0

Answer: (SHOW ANSWER)

----------R1---------- interface Ethernet0/0 ip address 209.165.201.1 255.255.255.0 ip access-group EGRESS2 out ipv6 address 2001:DB8::1/64 end

----------R2---------- interface Ethernet0/0 ip address 209.165.201.25 255.255.255.0 ipv6 address 2001:DB8::2/64 ipv6 address autoconfig ipv6 nd autoconfig default-route ipv6 nd cache expire 60 ipv6 nd ra suppress ipv6 traffic-filter INGRESS in end IOU_Router2#telnet 2001:DB8::1 Trying 2001:DB8::1 ... Open IOU_Router1>

NEW QUESTION: 15

The network administrator must implement IPv6 in the network to allow only devices that not only have registered IP addresses but are also connecting from assigned locations. Which security feature must be implemented?

A. IPv6 Router Advertisement Guard

B. IPv6 Destination Guard

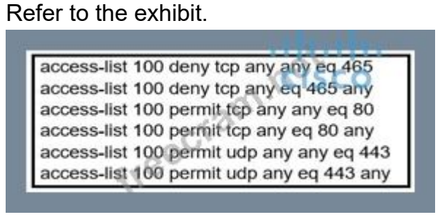
C. IPv6 Snooping

D. IPv6 Prefix Guard

Answer: (SHOW ANSWER)

NEW QUESTION: 16

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?

A. permit tcp port 443

B. permit tcp port 465

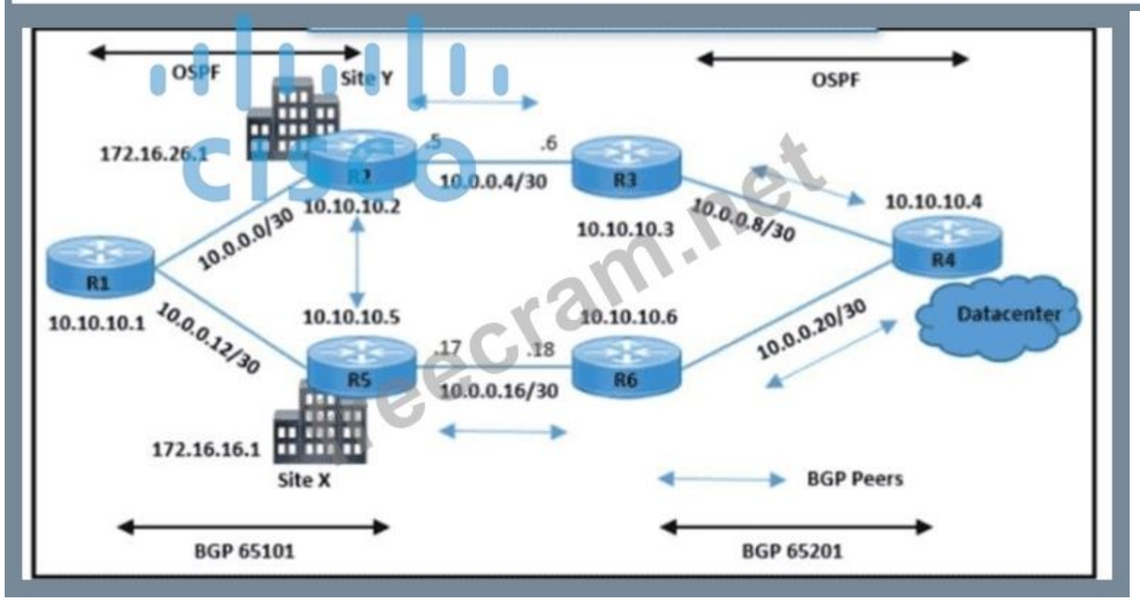
C. permit tcp port 22

D. permit udp port 465

Answer: (SHOW ANSWER)

NEW QUESTION: 17

```
R5#
*Sep 19 08:29:51.088: BGP: 10.10.10.2 open active, local address 10.0.0.14
*Sep 19 08:29:51.120: BGP: 10.10.10.2 read request no-op
*Sep 19 08:29:51.124: BGP: 10.10.10.2 open failed: Connection refused by
remote host, open active delayed 12988ms (20000ms max, 60% jitter)

R2#show  ip bgp neighbors 10.10.10.5
BGP neighbor is 10.10.10.5,  remote AS 65101, internal link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:01:18, last write 00:01:18, hold time is 15, keepalive
interval is 3 seconds
  Configured hold time is 15, keepalive interval is 3 seconds
  Minimum holdtime from neighbor is 0 seconds
  Address tracking is enabled, the RIB does have a route to 10.10.10.5
  Connections established 13; dropped 13
  Last reset 00:01:18, due to User reset
  Transport(tcp) path-mtu-discovery is enabled
  No active TCP connection
```



Refer to the exhibit A customer reported a failure and intermittent disconnection between two office buildings site X and site Y The network team finds that site X and site Y are exchanging email application traffic with the data center network Which configuration resolves the issue between site X and site Y?

A. RC(config)# ip prefix-list Customer seq 5 permit 192.168.30.1/32

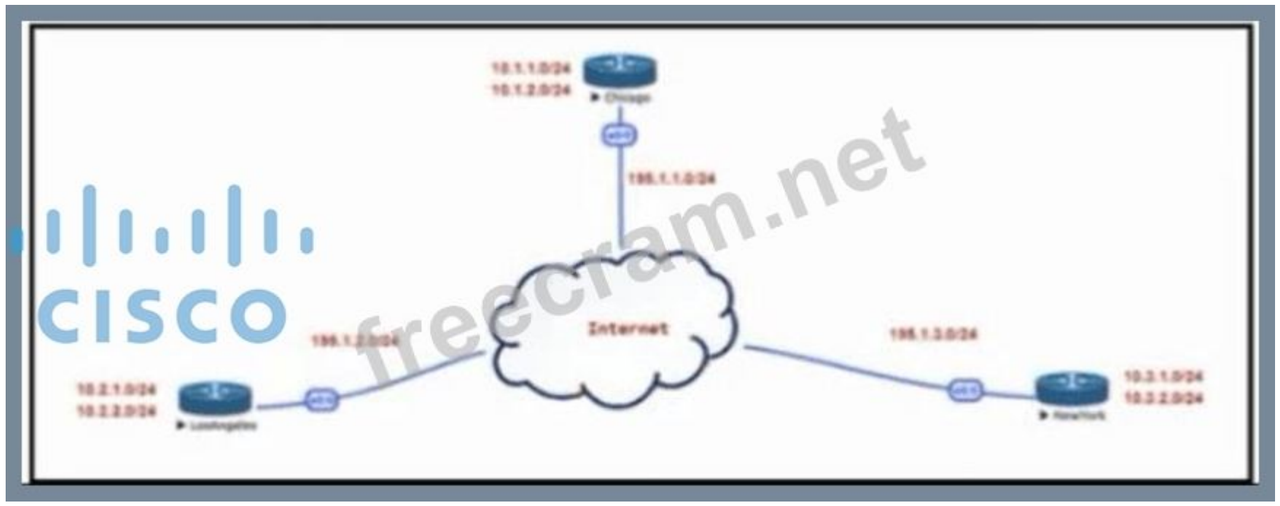
B. RF(config)#no ip prefix-list Customer seq 5 deny 192.168.1.1/32

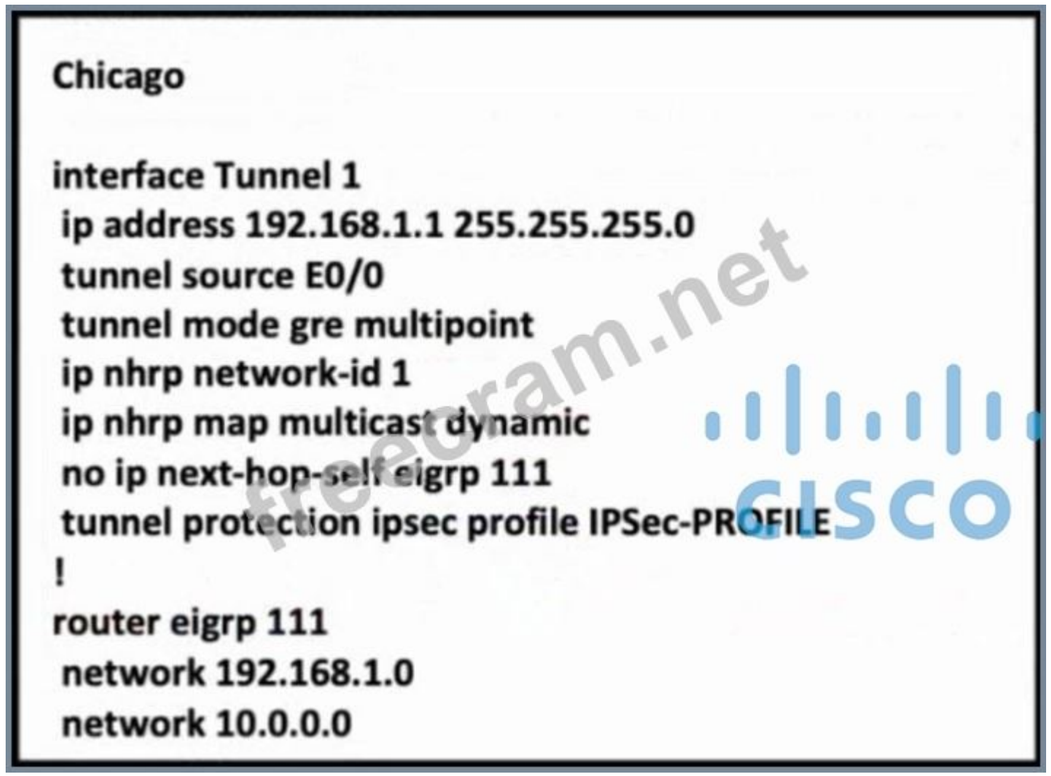
C. RF(config)#router bgp 65201
RF(config-router)# neighbor 10.0.0.17 prefix-list Customer out

D. RC(config)#router bgp 65101
RC(config-router)# neighbor 10.0.0.18 prefix-list Customer in

Answer: (SHOW ANSWER)

NEW QUESTION: 18





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?

A. Interface Tunnel1no ip split-horizon eigrp 111

B. Interface Tunnel1Ip next-hop-self elgrp 111

C. Interface Tunnel1tunnel mode Ipsec Ipv4

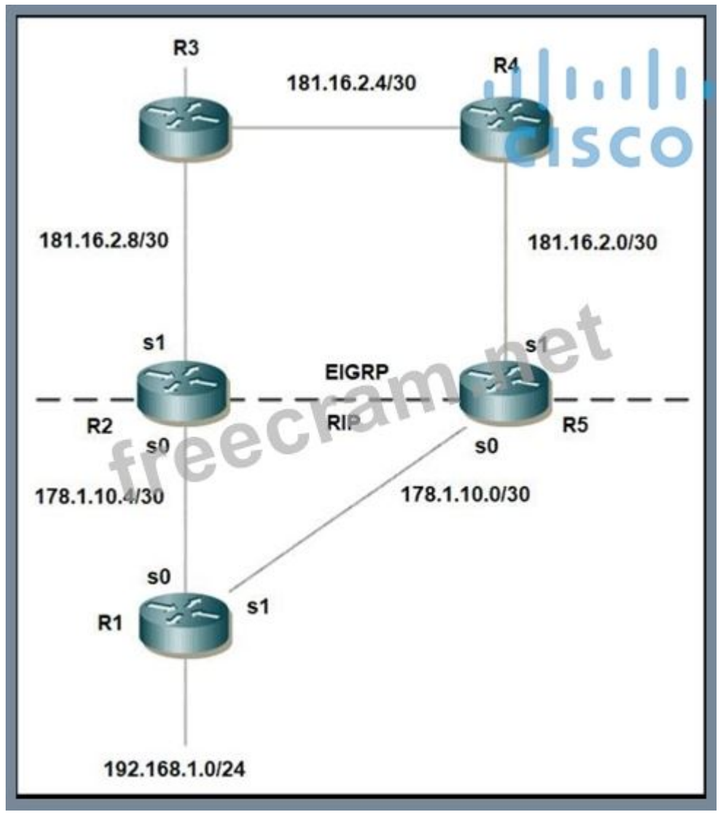
D. Interface Tunnel1tunnel protection ipsec profile IPSec-PROFILE

Answer: (SHOW ANSWER)

In this topology, Chicago router (Hub) will receive advertisements from Los Angeles (Spoke1) router on its tunnel interface. The problem here is that it also has a connection with New York (Spoke2) on that same tunnel interface. If we don't disable EIGRP split-horizon, then the Hub will not relay routes from Spoke1 to Spoke2 and the other way around. That is because it received those routes on interface Tunnel1 and therefore it cannot advertise back out that same interface (splithorizon rule). Therefore we must disable split-horizon on the Hub router to make sure the Spokes know about each other.

NEW QUESTION: 19

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?

A. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit any

B. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit any

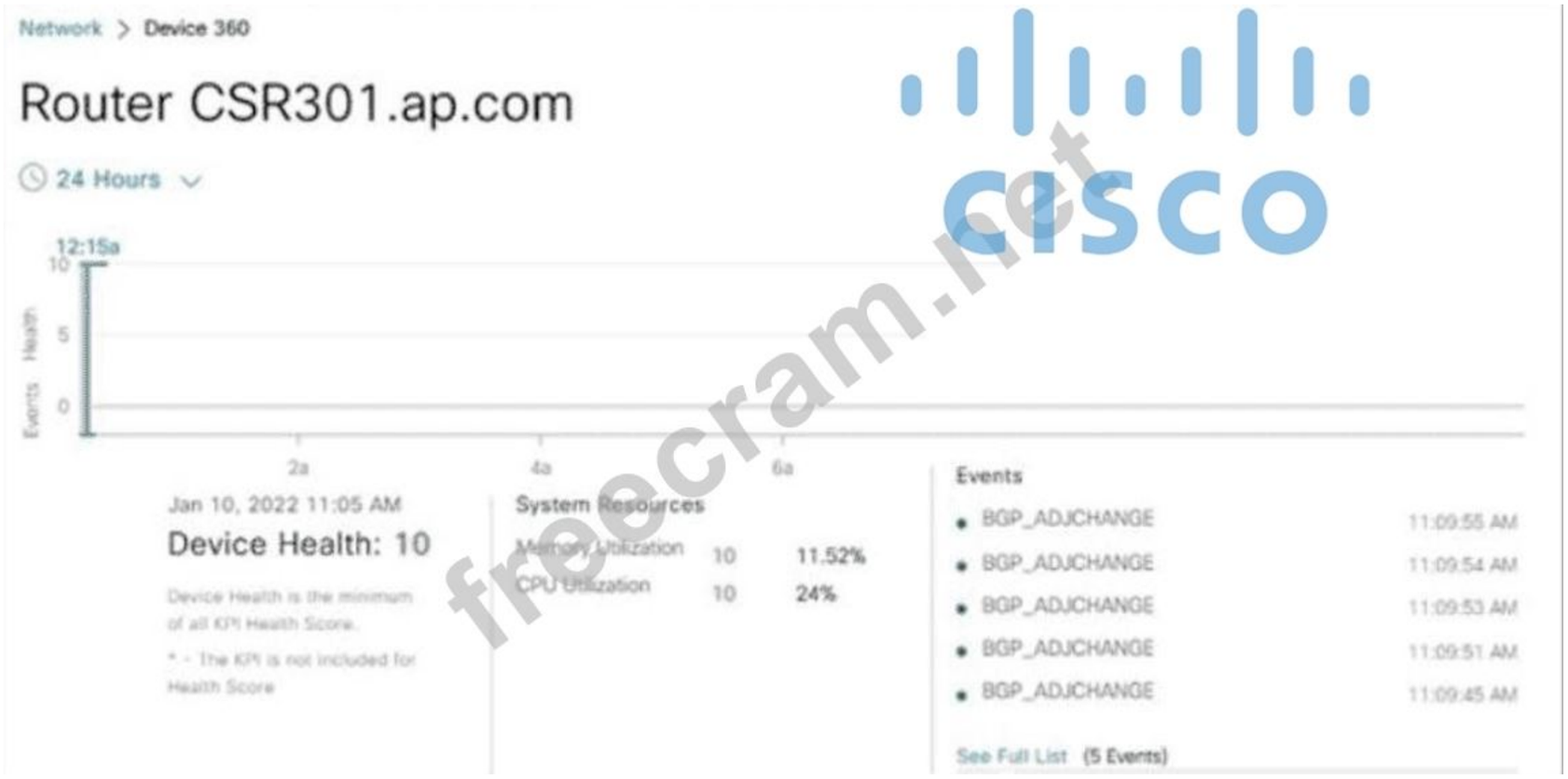
C. R2:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s0!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit anyR5:router eigrp 10network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 10 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit any

D. R2:router eigrp 7network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 7 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit anyR5:router eigrp 7network 181.16.0.0redistribute rip metric 1 1 1 1 1distribute-list 1 in s1!router ripnetwork 178.1.0.0redistribute eigrp 7 metric 2!access-list 1 deny 192.168.1.0access-list 1 permit any

Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.
html

NEW QUESTION: 20



```
atomic-aggregate, best
      Extended Community: RT:1:4099
      rx pathid: 0, tx pathid: 0x0
      Updated on Jul 28 2022 15:17:49 UTC

router#

router#sh ip bgp 10.140.217.0/24
% Network not in table
router#

router#sh ip bgp 10.140.217.0/24
BGP routing table entry for 10.140.217.0/24, version 685
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     5           11
  Refresh Epoch 1
  65396, (aggregated by 65396 10.140.210.2), imported path from
1:4099:10.140.217.0/24 (Guest_VN)

    10.140.212.5 from 10.140.212.5 (10.140.210.2)
      Origin IGP, metric 0, localpref 100, valid, external,
atomic-aggregate, best
      Extended Community: RT:1:4099
      rx pathid: 0, tx pathid: 0x0
      Updated on Jul 31 2022 18:32:12 UTC
```

Refer to the exhibit. In Cuco DNA Center, a network engineer identifies that BGP-learned networks are repeatedly withdrawn from peers. Which configuration must the engineer apply to resolve the Issue?

A.

```
router bgp 100
 bgp dampening
```

B.

```
route-map Dampening permit 10
 set dampening 15 750 2000 60
router bgp 100
 neighbor 10.140.212.5 route-map Dampening out
```

C.

```
route-map Dampening permit 10
 set dampening 15 750 2000 60
router bgp 100
 neighbor 10.140.212.5 route-map Dampening in
```

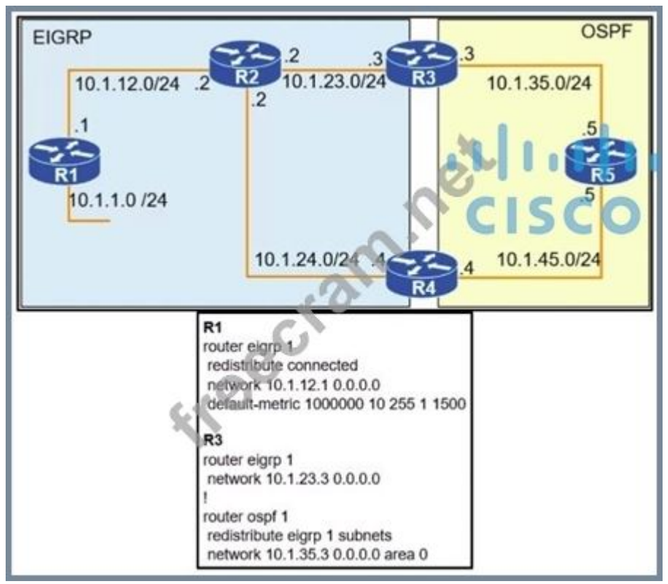
D.

```
router bgp 100
 bgp graceful-restart
```

Answer: (SHOW ANSWER)

NEW QUESTION: 21

Refer to the exhibit.



To provide reachability to network 10.1.1.0 /24 from R5, the network administrator redistributes EIGRP into OSPF on R3 but notices that R4 is now taking a ..... path through R5 to reach 10.1.1.0/24 network. Which action fixes the issue while keeping the reachability from R5 to 10.1.1.0/24 network?

A. Change the administrative distance of OSPF to 200 on R5.

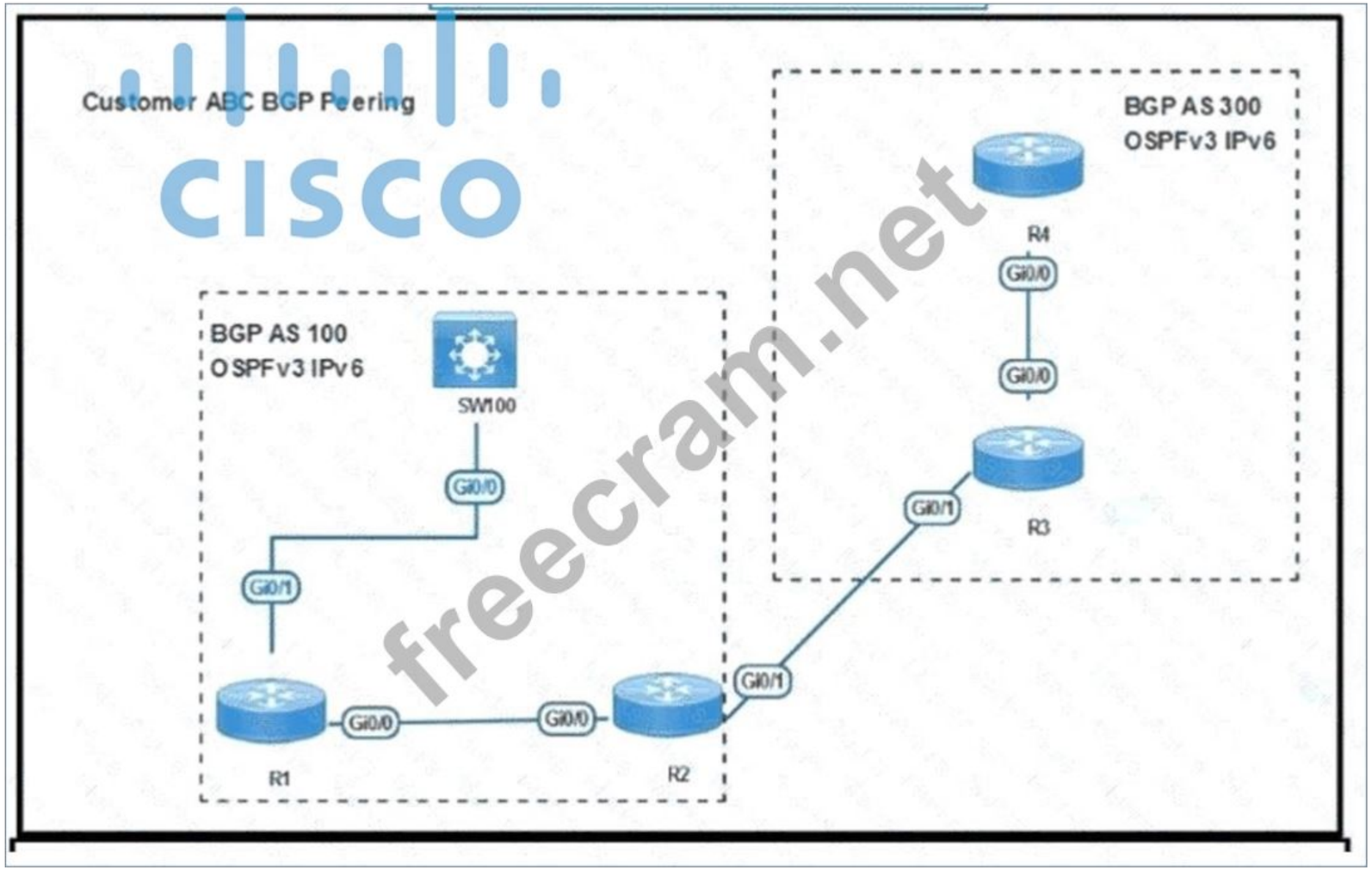
B. Apply the outbound distribution list on R5 toward R4 in OSPF.

C. Redistribute OSPF into EIGRP on R4

D. Change the administrative distance of the external EIGRP to 90.

Answer: (SHOW ANSWER)

NEW QUESTION: 22

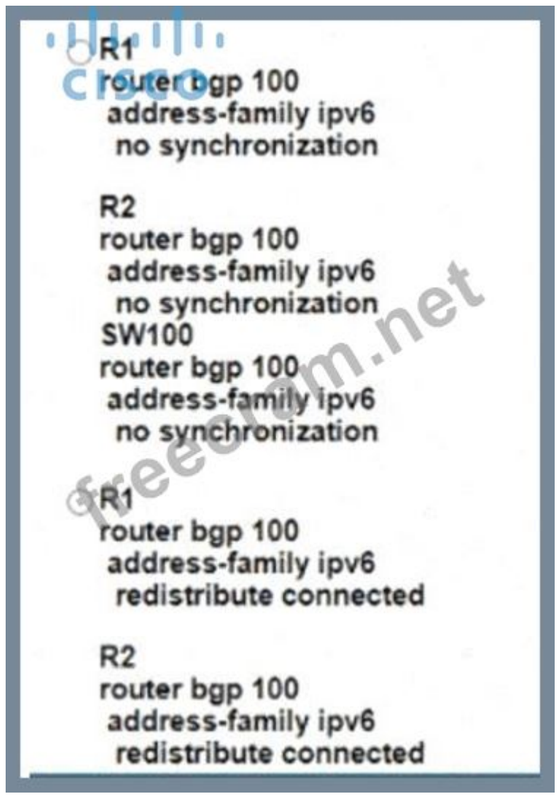

Customer ABC BGP Peering
BGP AS 100
OSPFv3 IPv6
SW100
Gi0/0
Gi0/1
Gi0/0
Gi0/0
R1
R2
BGP AS 300
OSPFv3 IPv6
R4
Gi0/0
Gi0/0
Gi0/1
R3
Gi0/1

```
SW100#sh ip bgp ipv6 uni summ
BGP router identifier 100.0.0.1, local AS number 100
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:ABC:AABB:1100:1122:1111:2222:AAA1
                4          100       6       5        1    0    0 00:00:58            0

SW100#sh ip bgp ipv6 unicast
SW100#

R1#sh ip bgp ipv6 uni
BGP table version is 4, local router ID is 1.1.1.1
     Network          Next Hop            Metric LocPrf Weight Path
 * i  2001::4/128     2001::4                  0    100      0 300 i
 *>i  2002::2/128     2001::2                  0    100      0 i
R1#
R1#sh ipv6 route
O   2001::2/128 [110/1]
     via FE80::5200:C3FF:FE01:E600, GigabitEthernet0/0
B   2002::2/128 [200/0]
     via 2001::2
```


Refer to the exhibit SW100 cannot receive routes from R1 Which configuration resolves the issue?

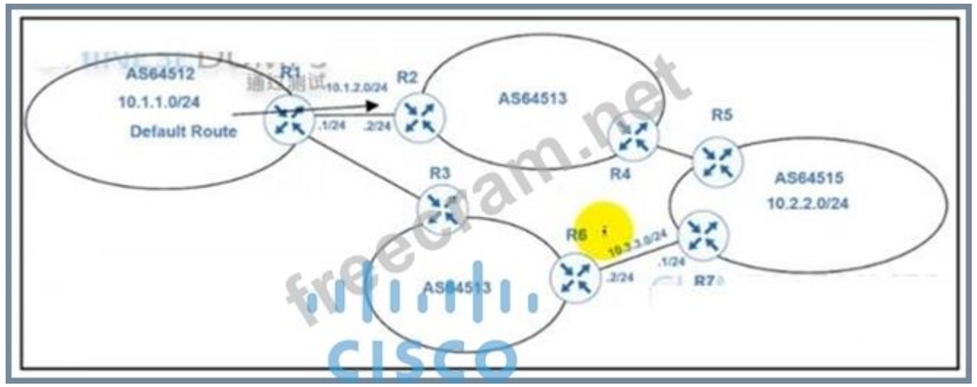
○ R1
```
router bgp 100
 address-family ipv6
  neighbor 2001::2 route-reflector-client
  neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client

R2
router bgp 100
 address-family ipv6
  neighbor 2001::2
  neighbor 2001::1 next-hop-self
```

○ R1
```
router bgp 100
 address-family ipv6
  neighbor 2001::2 route-reflector-client
  neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client

R2
router bgp 100
 address-family ipv6
  neighbor 2001::2
  neighbor 2001::1 as-override
```



A. Option A
B. Option C
C. Option B
D. Option C
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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. Option B
B. Option D
C. Option C
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 24

Refer to the exhibit. 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 lower LOCAL_PREF to select as the best path.

B. Configure AS_PATH prepend for the current best path

C. Configure AS_PATH prepend for the desired best path

D. Configure higher MED to select as the best path.

Answer: (SHOW ANSWER)

NEW QUESTION: 25

```
CPE# show snmp mib ifmib ifindex detail
Description               ifIndex  Active  Persistent  Saved  TrapStatus
-------------------------------------------------------------------------
Loopback1                 8        yes     disabled    no     enabled
GigabitEthernet1          1        yes     disabled    no     enabled
GigabitEthernet3          3        yes     disabled    no     enabled
GigabitEthernet3.123      10       yes     disabled    no     disabled
VoIP-Null0                5        yes     disabled    no     enabled
Loopback0                 7        yes     disabled    no     enabled
Null0                     6        yes     disabled    no     enabled
Loopback2                 9        yes     disabled    no     enabled
GigabitEthernet4          4        yes     disabled    no     enabled
GigabitEthernet2          2        yes     disabled    no     enabled
```

Refer to the exhibit. After reloading the router an administrator discovered that the interface utilization graphs displayed inconsistencies with their previous history in the NMS. Which action prevents this issue from occurring after another router reload in the future?

A. Configure SNMP to use static OIDs referring to individual router interfaces

B. Configure SNMP interface index persistence on the router

C. Rediscover all the router interfaces through SNMP after the router is reloaded

D. Save the router configuration to startup-config before reloading the router

Answer: B (LEAVE A REPLY)

NEW QUESTION: 26

```
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Ethernet0/0 from
LOADING to FULL, Loading Done
%BGP-3-NOTIFICATION: received from neighbor 192.168.200.1
active 6/7 (Connection Collision Resolution) 0 bytes
%BGP-5-NBR_RESET: Neighbor 192.168.200.1 active reset (BGP
Notification received)
%BGP-5-ADJCHANGE: neighbor 192.168.200.1 active Down BGP
Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor 192.168.200.1 IPv4 Unicast
topology base removed from session  BGP Notification received
```

Refer to the exhibit. An engineer noticed that the router log messages do not have any information about when the event occurred. Which action should the engineer take when enabling service time stamps to improve the logging functionality at a granular level?

A. Configure the debug uptime option

B. Configure the timezone option

C. Configure the msec option

D. Configure the tog uptime option
Answer: (SHOW ANSWER)

NEW QUESTION: 27
What is the output of the following command:
show ip vrf
A. Show's routing protocol information associated with a VRF.
B. Show's default RD values
C. Displays IP routing table information associated with a VRF
D. Displays the ARP table (static and dynamic entries) in the specified VRF
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Refer to the exhibit.

```
R1#show run | begin line
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synohronous
 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#
```


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 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
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: (SHOW ANSWER)
https://community.cisco.com/t5/other-network-architecture/out-of-band-router-access/td-p/333295 The "transport output none" command prevents any protocol connection made from R1.
Therefore our SSH connection to 192.168.12.2 was refused. In order to fix this problem we can configure "transport output ssh" under "line console 0" of R1.
Note: The parameter "-l" specifies the username to log in as on the remote machine.

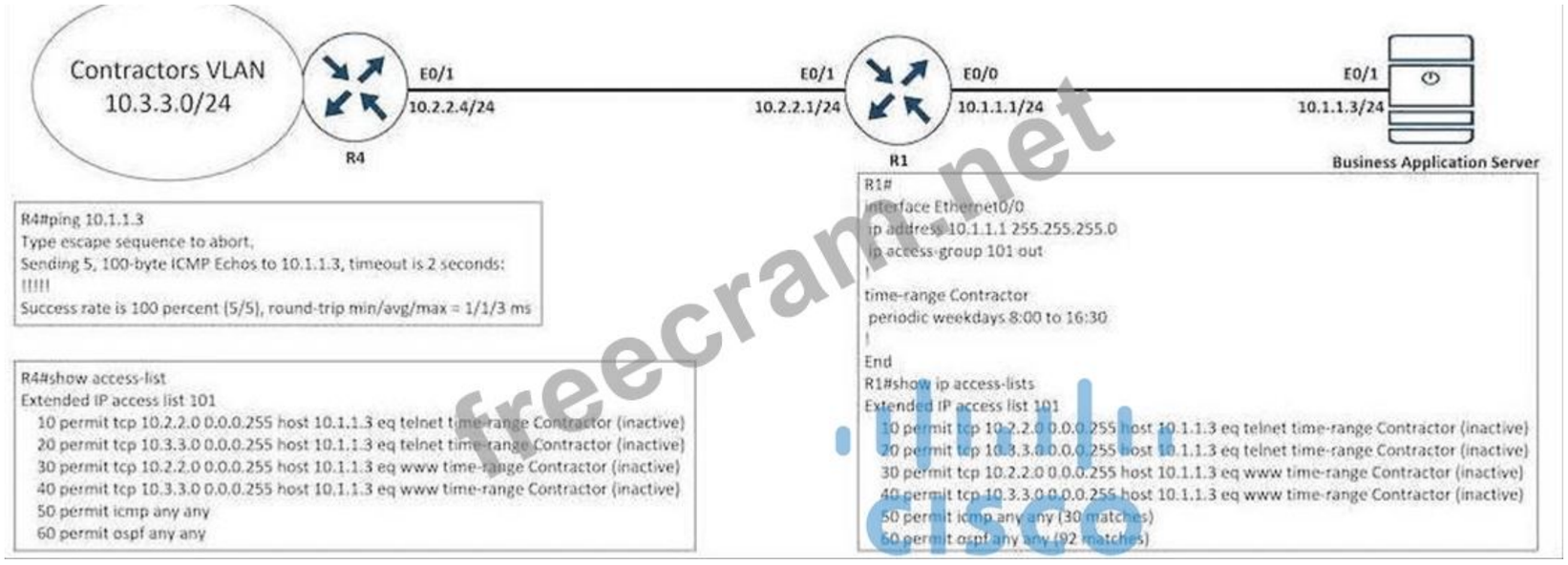
NEW QUESTION: 29
Refer to the exhibit.

```
Router#sh ip route ospf
<output omitted>
Gateway is last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
   o  E2     10.0.0.0 [110/20] via 192.168.12.2, 00:00:10, Ethernet0/0
   o       192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:50, 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#
```

An engineer is trying to redistribute OSPF to BGP, but not all of the routes are redistributed. What is the reason for this issue?
A. By default, only internal routes and external type 1 routes are redistributed into BGP

B. Only classful networks are redistributed from OSPF to BGP
C. BGP convergence is slow, so the route will eventually be present in the BGP table
D. By default, only internal OSPF routes are redistributed into BGP
Answer: D (LEAVE A REPLY)
If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default.
You can redistribute both internal and external (type-1 & type-2) OSPF routes via this command: #Router (config-router)#redistribute ospf 1 match internal external 1 external 2# Reference:
https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redis.
html

NEW QUESTION: 30
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
time-range Contractor
no periodic weekdays 17:00 to 23:59
periodic daily 8:00 to 16:30

B.
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

C.
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

D.
R1
time-range Contractor
no periodic weekdays 8:00 to 16:30
periodic daily 8:00 to 16:30

Answer: (SHOW ANSWER)

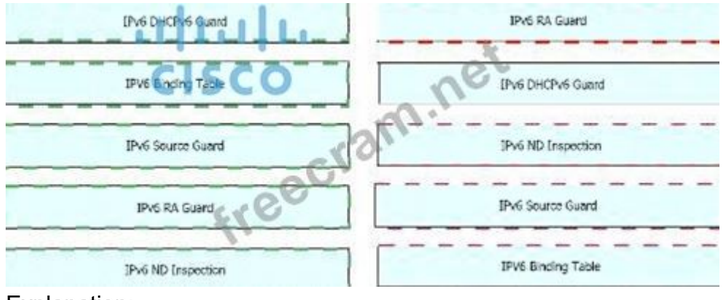
NEW QUESTION: 31
Which is statement about IPv6 inspection is true?
A. It learns and secures bindings for stateful autoconfiguration addresses in Layer 3 neighbor tables
B. It team and secures binding for stateless autoconfiguration addresses in Layer 2 neighbor tables.
C. It teams and secures bindings for stateless autoconfiguration addresses in Layer 3 neighbor tables
D. It teams and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables
Answer: (SHOW ANSWER)

NEW QUESTION: 32
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 no-registration
B. ip nhrp registration dynamic
C. ip nhrp registration no-unique
D. ip nhrp registration ignore
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which statement about IPv6 ND 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 stateless autoconfiguration addresses in Layer 2 neighbor tables.
C. It learns and secures bindings for stateful autoconfiguration addresses in Layer 3 neighbor tables.
D. It learns and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables.
Answer: (SHOW ANSWER)
IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages that do not have valid bindings are dropped. A neighbor discovery message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.
This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book
/ip6-snooping.pdf

NEW QUESTION: 34
Drag and Drop the IPv6 First-Hop Security features from the left onto the definitions on the right.

Answer:



Explanation:

Graphical user interface, chart Description automatically generated

NEW QUESTION: 35
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. test cable diagnostics tdr interface GigabitEthernet1/0/14
B. Check cable-diagnostics tdr interface GigabitEthernet1/0/14
C. show cable-diagnostics tdr interface GigabitEthernet1/0/14
D. Verify cable-diagnostics tdr interface GigabitEthernet1/0/14
Answer: (SHOW ANSWER)
The Time Domain Reflectometer (TDR) feature allows you to determine if a cable is OPEN or SHORT when it is at fault.
To start the TDR test, perform this task:
Step 1 (Starts the TDR test): test cable-diagnostics tdr {interface {interface-number}} Step 2 (Displays the TDR test counter information): show cable-diagnostics tdr {interface interface-number}
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-11/configuration_guide/int_hw/b_1611_int_and_hw_9600_cg/checking_port_status_and_connectivity pdf Text, table Description automatically generated

TDR test started on interface Gi1/0/14
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.

Wait 10 seconds and then issue the command to show the cable diagnostics result:

```
TDR test last run on: December 05 18:50:53
Interface Speed Local pair Pair length Remote pair Pair status
Gi1/0/14 1000M Pair A 19 +/- 10 meters Pair B Normal
               Pair B 19 +/- 10 meters Pair A Normal
               Pair C 19 +/- 10 meters Pair D Normal
               Pair D 19 +/- 10 meters Pair C Normal
```

Notice that the results are "Normal" in the above example. Other results can be:
+ Open: Open circuit. This means that one (or more) pair has "no pin contact".
+ Short: Short circuit.
+ Impedance Mismatched: Bad cable.

NEW QUESTION: 36

```
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 Ethernet0/0 203.0.113.1 name ISP1 track
!
ip route 0.0.0.0 0.0.0.0 Ethernet0/1 198.51.100.1 2 name ISP2
```

Refer to the exhibit. After recovering from a power failure. Ethernet0/1 stayed down while Ethernet0/0 returned to the up/up state The default route through ISP1 was not reinstated m the routing table until Ethernet0/1 also came up Which action resolves the issue?

A. Configure the default route through ISP1 with a higher administrative distance than 2.

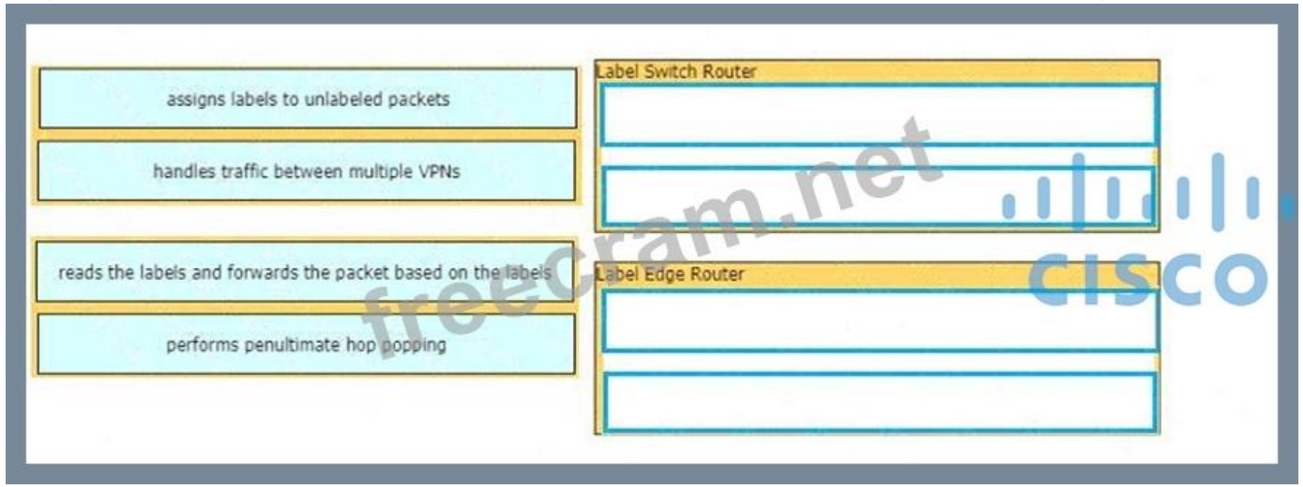
B. Reference the track object 1 in both static default routes

C. Add a static route to the 8 8.8 8/32 destination through the next hop 203.0.113.1

D. Remove the references to the interface names from both static default routes

Answer: (SHOW ANSWER)

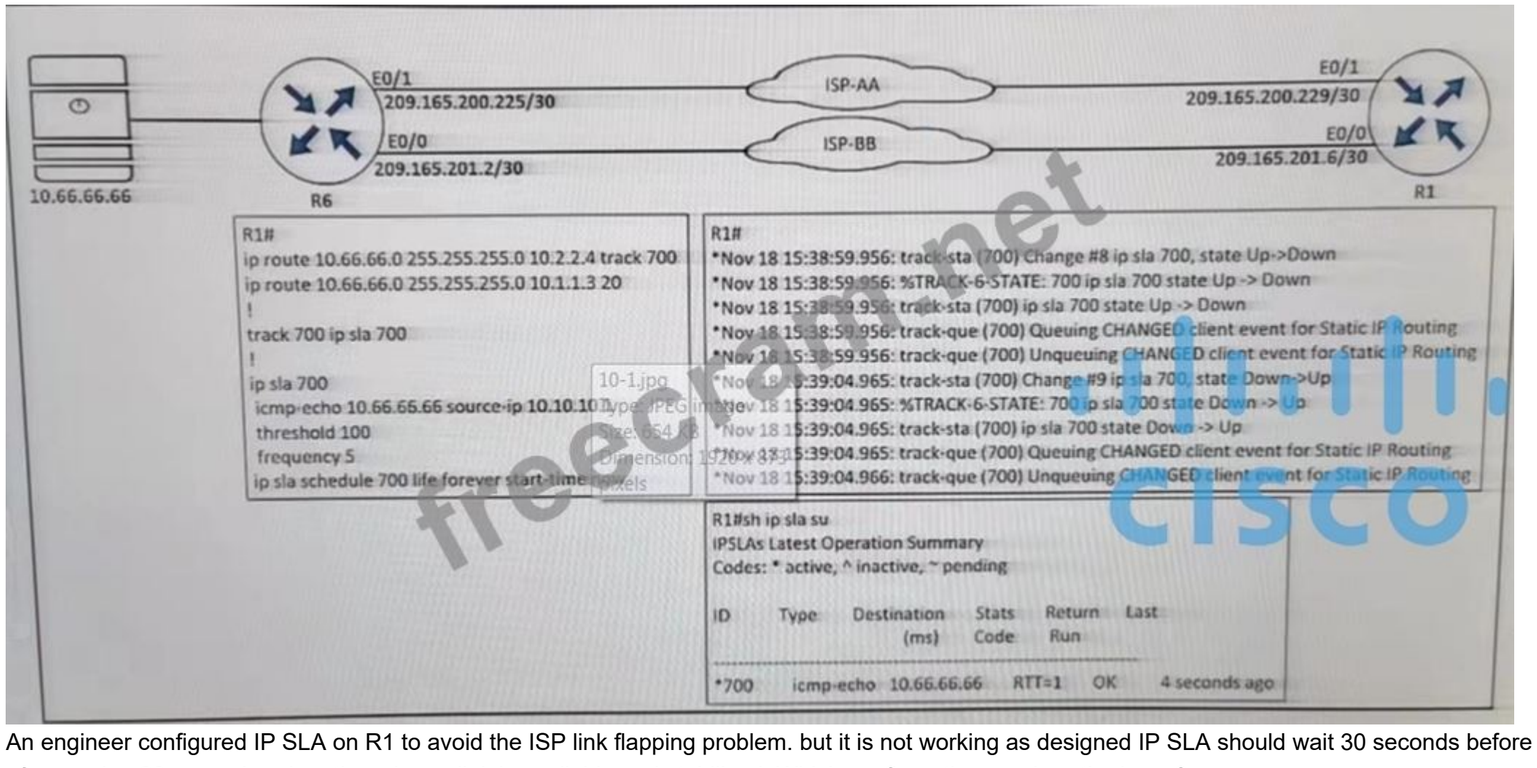
NEW QUESTION: 37
Drag and drop the operations from the left onto the locations where the operations are performed on the right.



Answer:

Explanation:
Label Switch Router 1. Reads labels and forwards the packet based on the based on the label.
2. Performs PHP
Label Edge Router: 1 Assigns labels and unlabeled packets.
2. Handles traffic between multiple VPNs

NEW QUESTION: 38
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 waning 20 seconds, when the primary link is available and stabilized. Which configuration resolves the issue?

A. R1(config)#ip sla 700R1(config-ip-sla)#delay down 30 up 20

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

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

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

Answer: (SHOW ANSWER)

"wait 30 seconds before switching traffic to a secondary connection" -> delay down 30

"then revert to the primary link after waiting 20 seconds" -> up 20

Under the track object, you can specify delays so we have to configure delay under "track 700 ip sla 700" (not under "ip sla 700").

NEW QUESTION: 39

Which routing protocol is used by the PE router to advertise routes to a CE router without redistribution or static after removing the RD tag from the P router?

A. MP-BGP

B. BGPIPv4

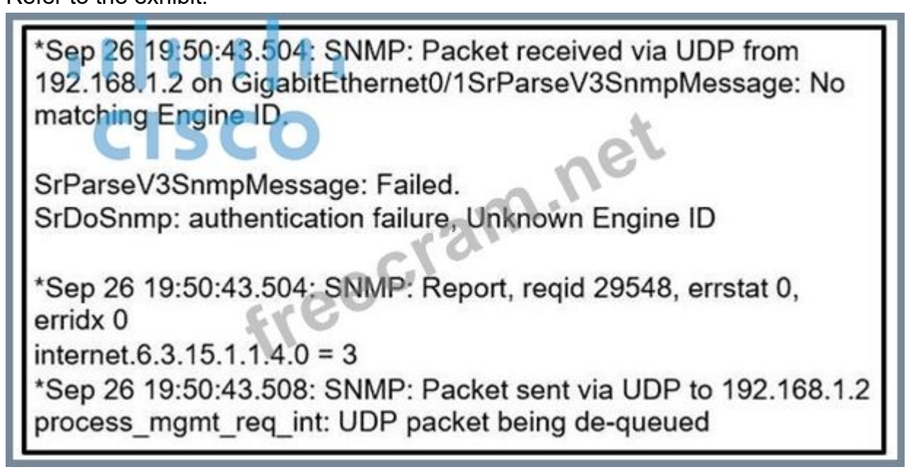
C. OSPF

D. IS-IS

Answer: (SHOW ANSWER)

NEW QUESTION: 40

Refer to the exhibit.



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

A. debug snmp packet

B. debug snmpv3 engine-id

C. debug snmp engine-id

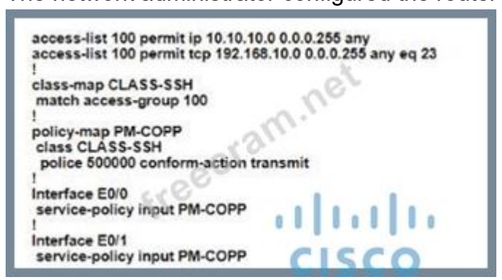
D. snmp user

E. showsnmpv3 user

Answer: (SHOW ANSWER)

NEW QUESTION: 41

The network administrator configured the router for Control Plane Policrg so that inbound SSH traffic is policed to 500 kbps This policy must apply to traffic coming in from 101010 0<24 and 192 168 10.0/24 networks



The Control Rane Policing is not applied to SSH traffic and SSH is open to use any bandwidth available.

Which configuration resolves this issue?

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
!
policy-map PM-COPP
 class CLASS-SSH
 no police 500000 conform-action transmit
 police 500000 conform-action transmit exceed-action drop
!
interface E0/0
 no service-policy input PM-COPP
!
interface E0/1
 no service-policy input PM-COPP
!
control-plane
 service-policy input PM-COPP
```

A.

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
!
policy-map PM-COPP
 class CLASS-SSH
 no police 500000 conform-action transmit
 police 500000 conform-action transmit exceed-action drop
```

B.

```
interface E0/0
 no service-policy input PM-COPP
!
interface E0/1
 no service-policy input PM-COPP
!
control-plane
 service-policy input PM-COPP
```

C.

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
```

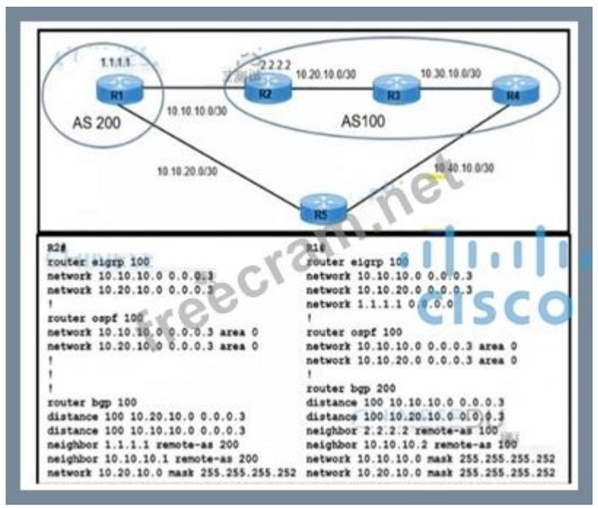
D.

```
no access-list 100
access-list 100 permit tcp 10.10.10.0 0.0.0.255 any eq 22
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22
!
Interface E0/0
 no service-policy input PM-COPP
!
Interface E0/1
 no service-policy input PM-COPP
!
control-plane
 service-policy input PM-COPP
```

Answer: (SHOW ANSWER)

NEW QUESTION: 42

Refer to the Exhibit.



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. Remove distance commands under BGP AS 100 and AS 200.

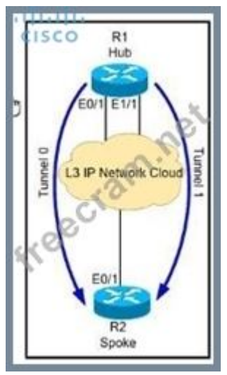
B. Remove distance commands under BGP AS 100.

C. Configure distance to 100 under the OSPF process of R1 and R2

D. Configure distance to 100 under the EIGRP process of R1 and R2.

Answer: (SHOW ANSWER)

NEW QUESTION: 43



Refer to me exhibit. The hub and spoke are connected 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

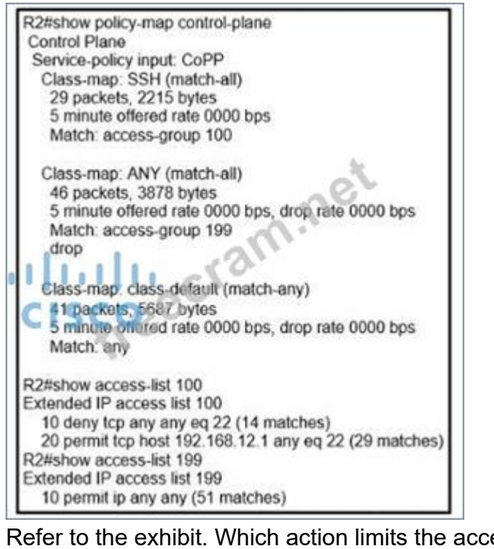
B. tunnel protection ipsec profile DMVPN tunnel1

C. tunnel protection ipsec profile DMVPN multipoint

D. tunnel protection ipsec profile DMVPN shared

Answer: (SHOW ANSWER)

NEW QUESTION: 44



Refer to the exhibit. Which action limits the access to R2 from 192.168.12.1?

A. Modify sequence 10 to deny tcp any eq 22 any to access-list 100.

B. Swap sequence 20 with sequence 10 in access-list 100

C. Swap sequence 10 with sequence 20 in access-list 100.

D. Modify sequence 20 to permit tcp host 192.168.12.1 eq 22 any to access-list 100

Answer: (SHOW ANSWER)

NEW QUESTION: 45

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

A. All VRFs share customers routing and CEF tables .

B. An interface must be associated to one VRF.

C. Each VRF has a different set of routing and CEF tables

D. It is defined by the VPN membership of a customer site attached to a P device.

E. A customer site can be associated to different VRFs

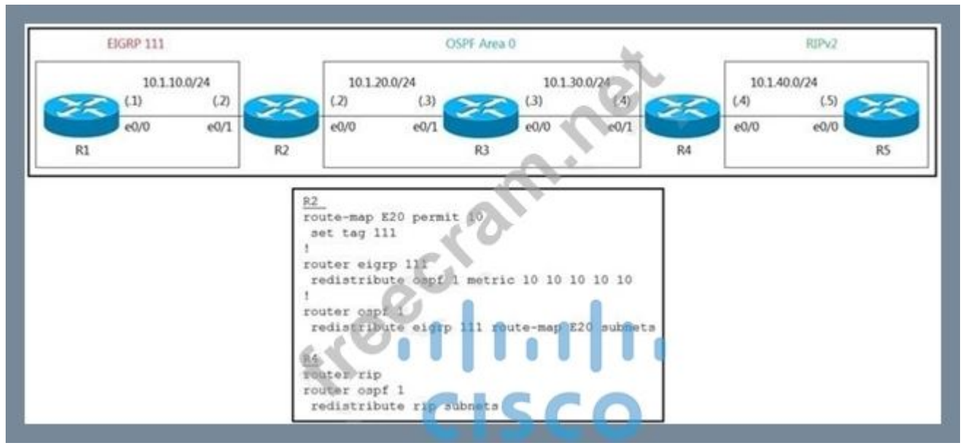
Answer: B,C (LEAVE A REPLY)

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xe-3s/isw-cef-xe-3s- book/isw-cef-basic-config.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-s/mp-l3-vpns-15-s-book/mp- bgp-mpls-vpn.pdf

NEW QUESTION: 46

Refer to the exhibit.



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?

A. R4route-map O2R deny 10match tag 111route-map O2R permit 20!router ripredistribute ospf 1 route- map O2R metric 1

B. R2route-map E20 deny 20R4route-map O2R deny 10match tag 111!router ripredistribute ospf 1 route- map O2R metric 1

C. R4route-map O2R permit 10match tag 111route-map O2R deny 20!router ripredistribute ospf 1 route- map O2R metric 1

D. R4route-map O2R deny 10match tag 111!router ripredistribute ospf 1 route-map O2R metric 1

Answer: (SHOW ANSWER)

In this question, routes from EIGRP domain are redistributed into OSPF (with tag 111) then RIPv2 but without any filtering so R5 learns all routes from both EIGRP and OSPF domain. If we only want R5 to learn routes from OSPF domain then we must filter out routes with tag 111 and permit other routes.

The line "route-map O2R permit 20" is important to allow other routes because of the implicit deny all at the end of each route-map.

NEW QUESTION: 47

```
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?

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

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 48

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.

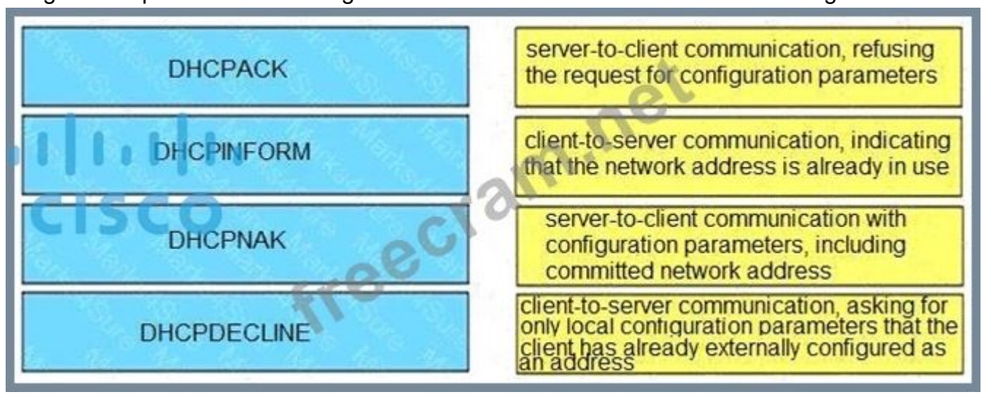
Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-ra- guard.html#GUID-589AF00C-7499-439F-AD23-51005D61CAB7 The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.

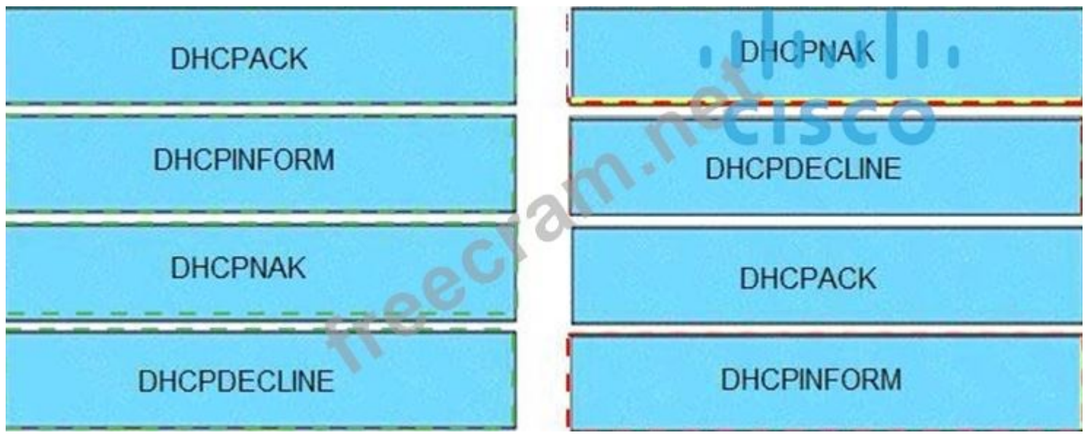
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6f-xe-16- book/ip6-ra-guard.pdf

NEW QUESTION: 49

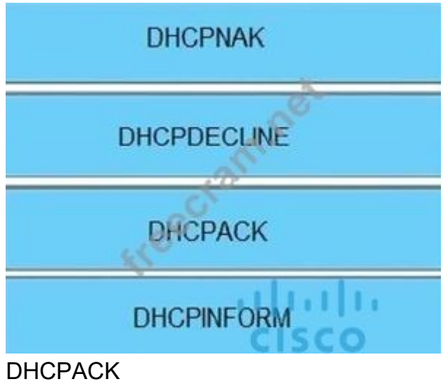
Drag and drop the DHCP messages from the left onto the correct uses on the right.



Answer:



Explanation:



DHCPACK

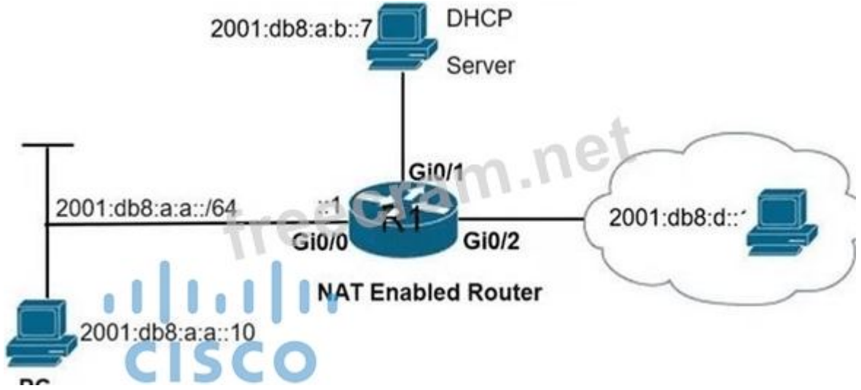
The server-to-client communication with configuration parameters, including committed network address.

DHCPINFORM

The client-to-server communication, asking for only local configuration parameters that the client already has externally configured as an address.

DHCPNAK
The server-to-client communication, refusing the request for configuration parameter.
DHCPDECLINE
The client-to-server communication, indicating that the network address is already in use Reference: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.
html
DHCPINFORM: If a client has obtained a network address through some other means or has a manually configured IP address, a client workstation may use a DHCPINFORM request message to obtain other local configuration parameters, such as the domain name and Domain Name Servers (DNSs). DHCP servers receiving a DHCPINFORM message construct a DHCPACK message with any local configuration parameters appropriate for the client without allocating a new IP address. This DHCPACK will be sent unicast to the client.
DHCPNAK: If the selected server is unable to satisfy the DHCPREQUEST message, the DHCP server will respond with a DHCPNAK message. When the client receives a DHCPNAK message, or does not receive a response to a DHCPREQUEST message, the client restarts the configuration process by going into the Requesting state. The client will retransmit the DHCPREQUEST at least four times within 60 seconds before restarting the Initializing state.
DHCPACK: After the DHCP server receives the DHCPREQUEST, it acknowledges the request with a DHCPACK message, thus completing the initialization process.
DHCPDECLINE: The client receives the DHCPACK and will optionally perform a final check on the parameters. The client performs this procedure by sending Address Resolution Protocol (ARP) requests for the IP address provided in the DHCPACK. If the client detects that the address is already in use by receiving a reply to the ARP request, the client will send a DHCPDECLINE message to the server and restart the configuration process by going into the Requesting state.
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html

NEW QUESTION: 50
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 20 for sequence 40 in the access list to allow Telnet.

B. Remove sequence 30 and add it back to the IPv6 traffic filter as sequence 5.

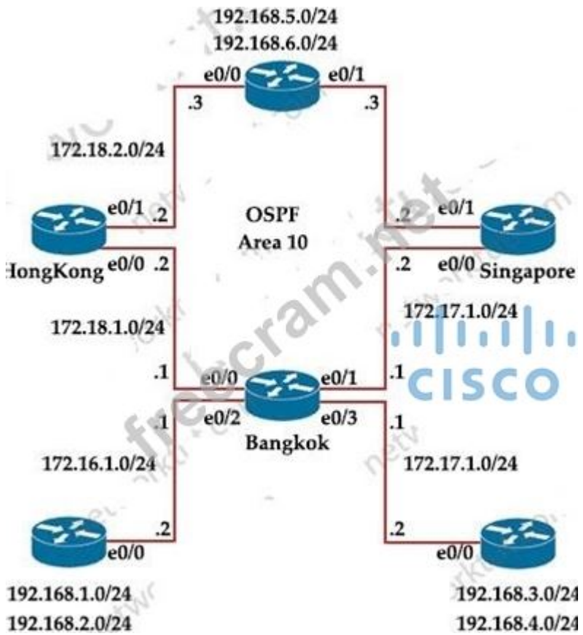
C. Remove sequence 20 and add it back to the IPv6 traffic filter as sequence 5.

D. Remove sequence 10 to add the PC source IP address and add it back as sequence 10.

Answer: (SHOW ANSWER)

NEW QUESTION: 51

Exhibit:



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 and192.168.4.0/24 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 0.0.0.255access-list 101 permit tcp
192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255!route-map PBR1 permit 10match ip address 101set ip next- hop 172.18.1.2interface Ethernet0/3ip 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 23access-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 10match ip address 101set ip next-hop 172.18.1.2interface Ethernet0/1ip 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 23access-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 10match ip address 101set ip next-hop 172.18.1.2!interface Ethernet0/3ip policy route-map PBR1

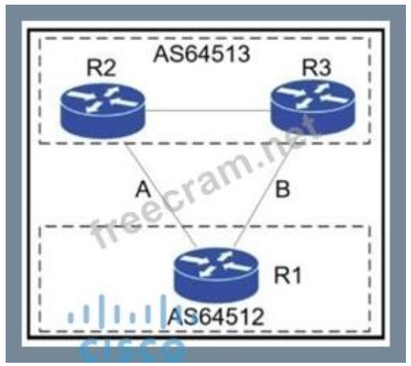
D. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255access-list 101 permit tcp
192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255!route-map PBR1 permit 10match ip address 101set ip next- hop 172.18.1.2!interface Ethernet0/1ip policy route-map PBR1

Answer: (SHOW ANSWER)

We need to use Policy Based Routing (PBR) here on Bangkok router to match the traffic from 192.168.3.0/24
& 192.168.4.0/24 and "set ip next-hop" to HongKong router(172.18.1.2 in this case).
Note: Please notice that we have to apply the PBR on incoming interface e0/3 to receive traffic from
192.168.3.0/24 and 192.168.4.0/24.

NEW QUESTION: 52

Refer to the exhibit.



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

Which BGP configuration on R1 accomplishes this goal?

A.
```
route-map link-a-in permit 10
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
```

B.
```
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
```

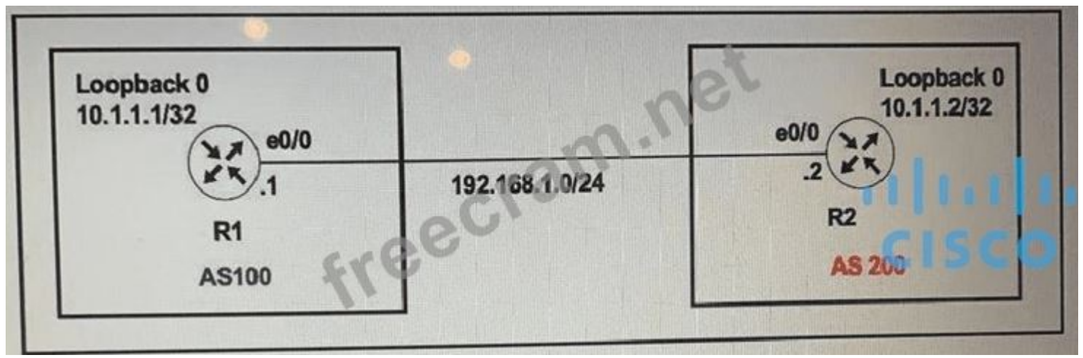
C.
```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
 set as-path prepend 64512
```

D.
```
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
```

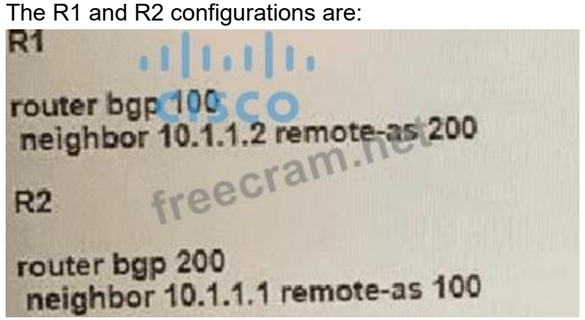
Answer: (SHOW ANSWER)

NEW QUESTION: 53

Refer to the exhibit.



The R1 and R2 configurations are:



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

A. R2ip route 10.1.1.1 255.255.255.255 192.168.1.1#router bgp 200neighbor 10.1.1.1 tti-security hops
1neighbor 10.1.1.1 update-source loopback 0

B. R2ip route 10.1.1.1 255.255.255.255 192.168.1.1#router bgp 200neighbor 10.1.1.1 disable-connected- checkneighbor 10.1.1.1 update-source loopback 0

C. R2ip route 10.1.1.2 255.255.255.255 192.168.1.2#router bgp 100neighbor 10.1.1.2 ttl-security hops
1neighbor 10.1.1.2 update-source loopback 0

D. R1ip route 10.1.1.2 255.255.255.255 192.168.1.2#router bgp 100neighbor 10.1.1.1 ttl-security hops
1neighbor 10.1.1.2 update-source loopback 0

E. R1ip route 10.1.1.2 255.255.255.255 192.168.1.2#router bgp 100neighbor 10.1.1.2 disable-connected- checkneighbor 10.1.1.2 update-source Loopback0

Answer: (SHOW ANSWER)

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.

Disable-connected-check enables a directly connected eBGP neighbor to peer using a loopback address without adjusting the default TTL of 1. In disable connected check the router does not decrease the TTL of an IP packet that is destined to itself so it only counts or considers as one hop between the two loopbacks of the routers.

NEW QUESTION: 54

Which router translates the customer routing information into VPNv4 routes to exchange VPNv4 routes with other devices through MP-BGP?

A. P

B. PE

C. VPNv4 RR

D. CE
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
Which two features are required for MPLS forwarding on which types of routers? (Choose two.)
A. MPLS on CE and core routers
B. MPLS on PE and core routers
C. LDP on PE and core routers
D. LDP on PE and CE routers
E. CEF on PE and CE routers
Answer: (SHOW ANSWER)

NEW QUESTION: 56
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. Clear the logical interfaces with snmp ifindex clear command
B. Trigger a new snmpwalk from the monitoring system to synchronize interface OIDs
C. Configure the snmp ifindex persist command globally.
D. Configure the snmp ifindex persist command on the physical interfaces.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
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
```

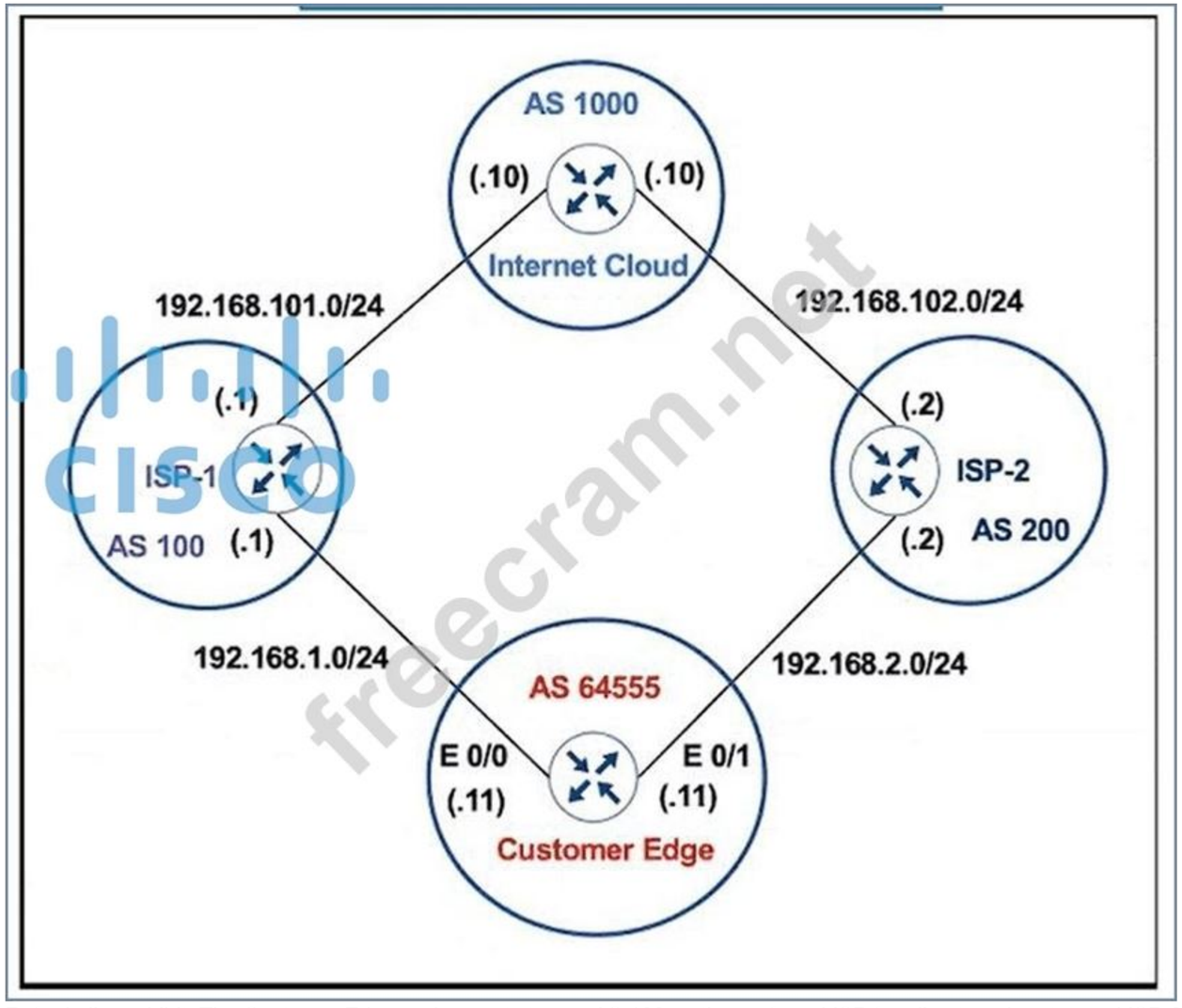
Desired

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

Answer: (SHOW ANSWER)

NEW QUESTION: 58



Refer lo lhe exhibit. The Customer Edge rouler wants to use AS 100 as the preferred ISP for all external routes and ISP-2 as a backup.

```
Customer-Edge

route-map SETAS
 set as-path prepend 111
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS in
```

After this configuration, all the backup routes have disappeared from the BGP table on the Customer Edge router. Which set of configurations resolves the issue on the Customer Edge router?

A.
```
route-map SETAS
 set as-path prepend 200
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS in
```

B.
```
route-map SETAS
 set as-path prepend 111
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS out
```

C.
```
route-map SETAS
 set as-path prepend 111
!
router bgp 64555
 neighbor 192.168.2.2 remote-as 100
 neighbor 192.168.1.1 remote-as 200
 neighbor 192.168.1.1 route-map SETAS in
```

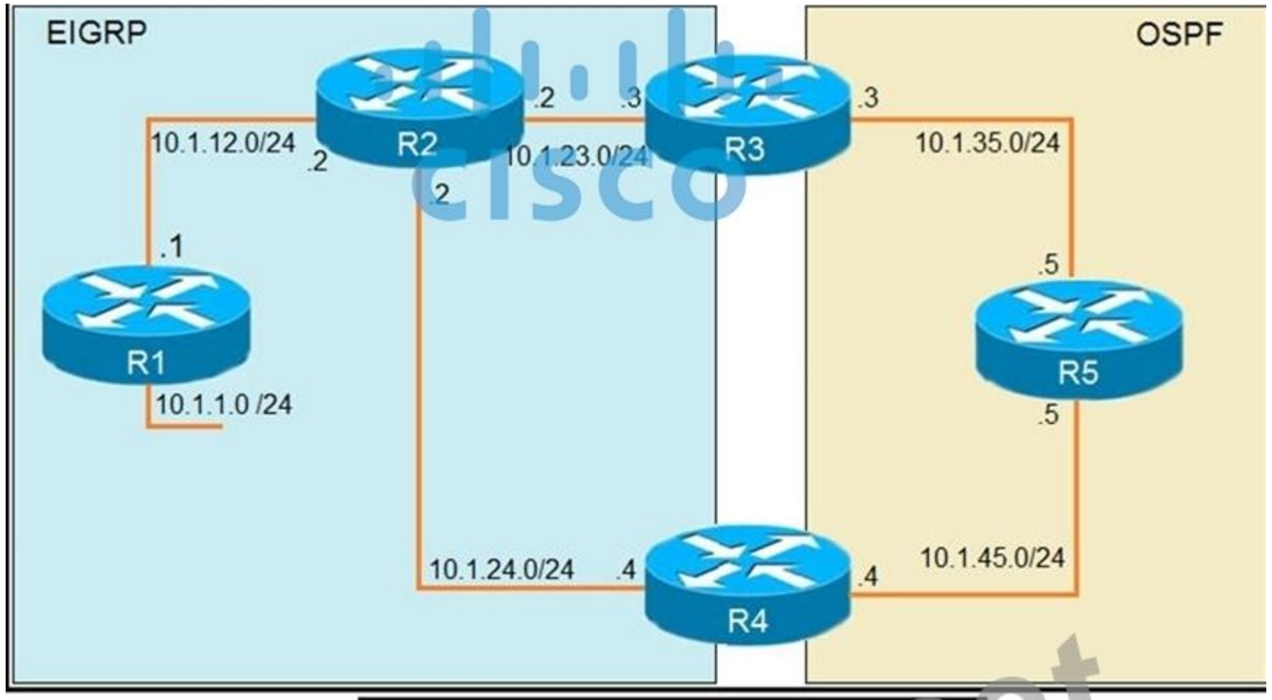
D.

```
route-map SETAS
 set as-path prepend 200
!
router bgp 64555
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.2.2 route-map SETAS out
```


Answer: (SHOW ANSWER)

NEW QUESTION: 59

Refer to the exhibit.




```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0

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

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

R5#traceroute 10.1.1.1

Type escape sequence to abort.
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 148 msec
6 10.1.23.2 108 msec 76 msec 80 msec
      <output truncuated>
```

The output of the trace route from R5 shows a loop in the network. Which configuration prevents this loop?

A.

```
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.

```
R3
router eigrp 1
 redistribute OSPF 1 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
```

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
 match tag 1

C.

```
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
```

D.

Answer: (SHOW ANSWER)

The reason for the loop is that R2 is forwarding the packets destined to 10.1.1.1 to R4, instead of R1. This is because in the redistribute OSPF statement, BW metric has a higher value and delay has a value of 1. So, R2 chooses R4 over R1 for 10.1.1.0/24 subnet causing a loop. Now, R5 learns 10.1.1.0/24 from R3 and advertises the same route to R4, that R4 redistributes back in EIGRP. If R3 sets a tag of 1 while redistributing EIGRP in OSPF, and R4 denies all the OSPF routes with tag 1 while redistributing, it will not advertise 10.1.1.0/24 back into EIGRP. Hence, the loop will be broken.

NEW QUESTION: 60

```
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?

A. Remove the prefix keyword from the distribute-list command.

B. Remove the line with the sequence number 10 from the prefix list.

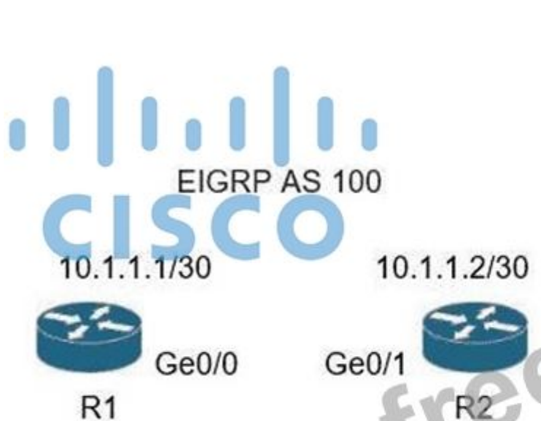
C. Remove the line with the sequence number 5 from the prefix list.

D. Change the direction of the distribute-list command from out to in.

Answer: (SHOW ANSWER)

NEW QUESTION: 61

Refer to the exhibit.




```
R1# debug eigrp packets
(UPDATE, REQUEST, QUERY, REPLY, HELLO,
UNKNOWN, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)
EIGRP Packet debugging is on
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
iidbQ un/rely 0/0
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
iidbQ un/rely 0/0
```


Which action resolves the adjacency issue?

A. Match the hello interval timers.

B. Configure the same EIGRP process IDs.

C. Match the authentication keys.

D. Configure the same autonomous system numbers.

Answer: (SHOW ANSWER)

EIGRP does not have process ID as it uses Autonomous System (AS) numbers only.

This is not an authentication problem or we would see this error from the debug:

EIGRP: Ethernet0/0: ignored packet from 10.1.1.3, opcode = 1 (missing authentication or key-chain missing) If the AS numbers between two routers are different then the neighbor relationship cannot be formed.

NEW QUESTION: 62

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 provides. 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 .*
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

C.
```
ip as-path access-list 1 permit ^45123$
!
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: (SHOW ANSWER)

By default BGP advertises all prefixes to external BGP neighbors. This means that if you are multi-homed (connected to two or more ISPs) then you might become a transit AS. For example, ISP 2 in AS 200 can send traffic to your router in AS 100 to reach ISP 3 in AS 300 because you advertised prefixes in ISP 3 to ISP 2.

This is what will be seen in the BGP routing table of ISP1:

```
ISP1#show ip bgp
--output omitted--
 Network          Next Hop            Metric LocPrf Weight Path
....
*> 3.3.3.0/24     192.168.12.1                           0 100 300 i
```


NEW QUESTION: 63

Refer to the exhibit.

```
nterface Ethernet0/1
no ip address
ipv6 address 2001:DB8:1:12::2/64
ipv6 traffic-filter ACL in

pv6 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

R# 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
enied icmpv6 2001:DB8:1:12::1 -> FF02::1:FF00:2 (135/0), 732
```

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. Change the next hop of the default route to the link-local address of the default gateway.

B. Enable the ND proxy feature on the default gateway.

C. Permit ICMPv6 neighbor discovery traffic in the ACL.
D. Remove the ACL entry 80.
E. Configure a link-local address on the Ethernet0/1 interface.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Refer to the exhibit.

```
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
```

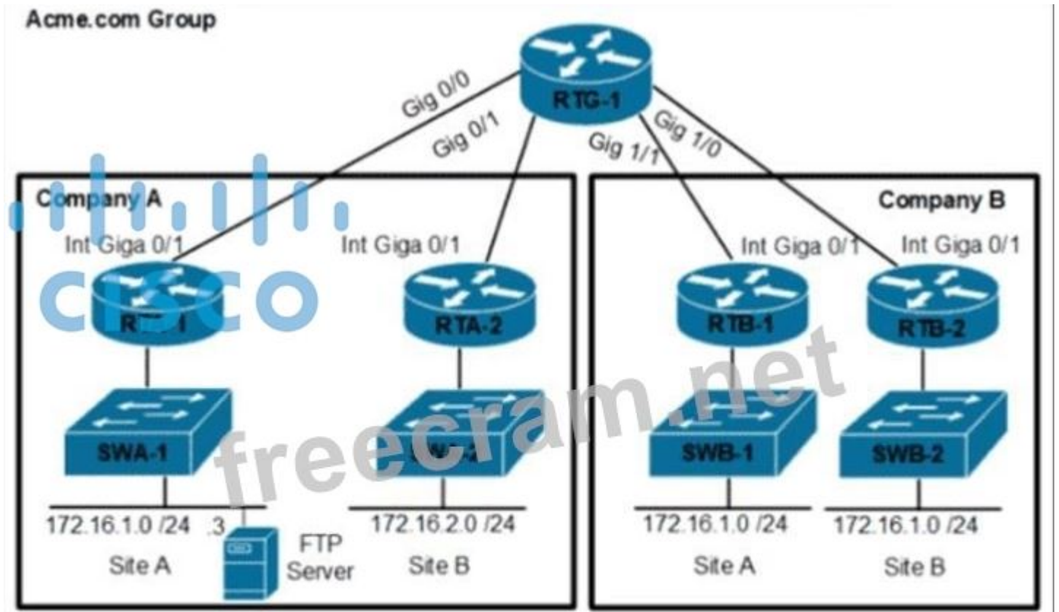
Which control plane policy limits BGP traffic that is destined to the CPU to 1 Mbps and ignores BGP traffic that is sent at higher rate?
A. policy-map LIMIT_BGP
B. policy-map SHAPE_BGP
C. policy-map COPP
D. policy-map POLICE_BGP
Answer: (SHOW ANSWER)

NEW QUESTION: 65
An engineer configured a DHCP server for Cisco IP phones to download its configuration from a TFTP server, but the IP phones failed to toad the configuration What must be configured to resolve the issue?
A. BOOTP port 67
B. DHCP option 66
C. BOOTP port 68
D. DHCP option 69
Answer: (SHOW ANSWER)

Command	Purpose
dhcpd option 66 ascii *server_name* **Example:** `hostname(config)# dhcpd option 66 ascii exampleserver`	Provides the IP address or name of a TFTP server for option 66.

DHCP options 3, 66, and 150 are used to configure Cisco IP Phones. Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, ifit does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.+ DHCP option 150 provides the IP addresses of a list of TFTP servers.+ DHCP option 66 gives the IP address or the hostname of a single TFTP server.
Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/basic_dhcp.
pdf

NEW QUESTION: 66




```
RTG-1(config)#ip vrf CompanyA
RTG-1(config-vrf)# interface GigabitEthernet 0/0
RTG-1(config-if)# ip vrf forwarding CompanyA
RTG-1(config-if)# ip address 172.16.2.2 255.255.255.0
```

Refer to the exhibit. An engineer must configure a per VRF for TACACS+ for company A.
Which configuration on RTG-1 accomplishes the task?

```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.1  port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/0
 ip vrf forwarding CompanyA
```

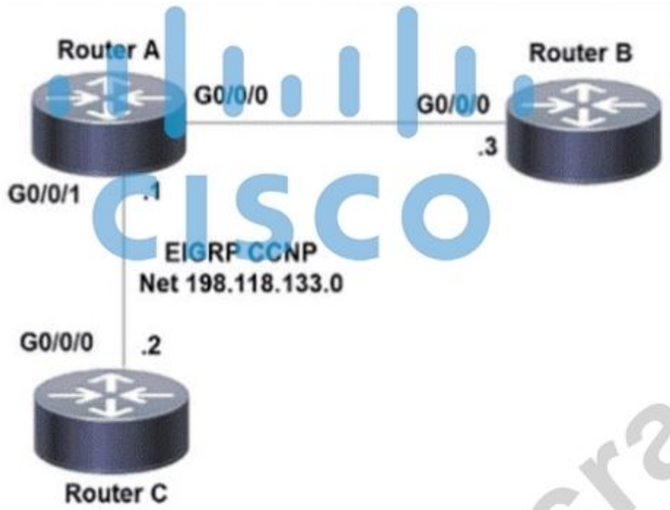
```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.3 port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/1
 ip vrf forwarding CompanyA
```

```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.1  port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/1
 ip vrf CompanyA
```

```
aaa new-model
aaa group server tacacs+ Tacacscluster
 server-private 172.16.1.3  port 49 key routing
 ip tacacs source-interface GigabitEthernet 0/0
 ip vrf CompanyA
```

A. Option D
B. Option C
C. Option A
D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 67




```
RouterA#sh ip eigrp interfaces gigabitEthernet 0/0/1
EIGRP-IPv4 Interfaces for AS(1)
                              Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface              Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
EIGRP-IPv4 VR(CCNP) Address-Family Interfaces for AS(100)
                              Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface              Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Gi0/0/1                  0        0/0          0/0        0        0/0           50           0
RouterA#
```

Refer to the exhibit EIGRP adjacency between router A and router C is not working as expected Which two configurations resolve the issue? (Choose two)

A.

```
Router C
router eigrp CCNP
 address-family ipv4 unicast autonomous-system 100
 af-interface GigabitEthernet0/0/0
  hold-time 90
 exit-af-interface
 topology base
 exit-af-topology
exit-address-family
```

Router A
router eigrp CCNP
 address-family ipv4 unicast autonomous-system 10
af-interface GigabitEthernet0/0/1
  hello-interval 15
  hold-time 90
 exit-af-interface
 topology base
 exit-af-topology
 network 198.18.133.0
exit-address-family

B.

Router A
router eigrp CCNP
 address-family ipv4 unicast autonomous-system 100
af-interface GigabitEthernet0/0/1
 hello-interval 15
topology base
exit-af-topology
network 192.18.133.0
exit-address-family

C.

Router C
router eigrp CCNP
  address-family ipv4 unicast autonomous-system 100
    topology base
    exit-af-topology
    network 198.18.133.0
  exit-address-family

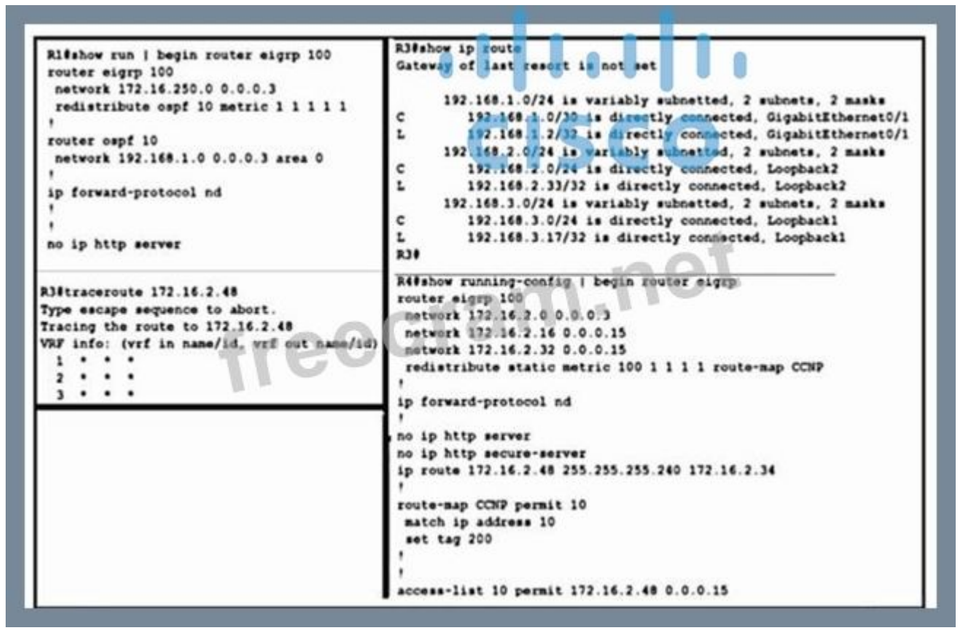
D.

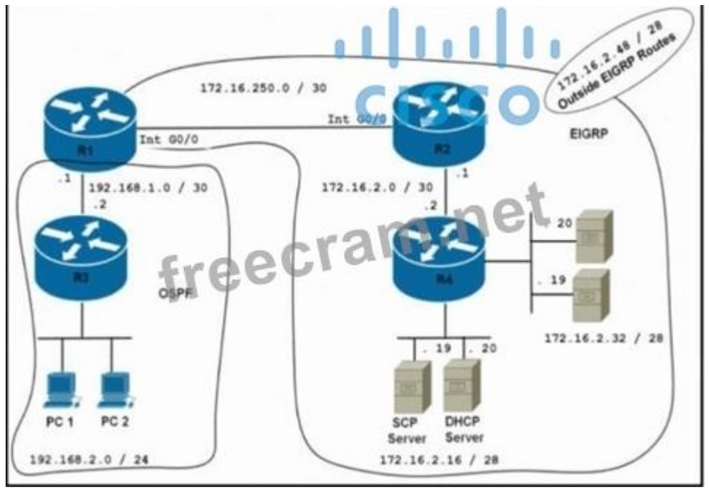
E.

```
Router A
router eigrp CCNP
  address-family ipv4 unicast autonomous-system 100
    topology base
    exit-af-topology
    network 198.18.133.0
  exit-address-family
```

Answer: (SHOW ANSWER)

NEW QUESTION: 68





Refer to the exhibit. An engineer must troubleshoot a connectivity issue impacting the redistribution of the subnet 172.16.2.48/28 into the OSPF domain. Which configuration on router R1 advertises this subnet into OSPF?

A. R1(config-router)#redistribute eigrp 100 subnets route-map CCNP
R1(config)#router ospf 10
R1(config-route-map)#match route-type internal
R1(config)#route-map CCNP permit 10

B. R1(config-router)#redistribute eigrp 100 subnets route-map CCNP
R1(config)#router ospf 10
R1(config-route-map)#exit
R1(config-route-map)#match tag 200
R1(config)#route-map CCNP permit 10

C. R1(config-router)#redistribute eigrp 100 subnets route-map CCNP
R1(config)#router ospf 10
R1(config-route-map)#match route-type level-2
R1(config)#route-map CCNP permit 10

D. R1(config-router)#redistribute eigrp 100 subnets route-map CCNP
R1(config)#router ospf 10
R1(config)#route-map CCNP permit 10
R1(config-route-map)#match tag 200
R1(config)#route-map CCNP deny 10

Answer: (SHOW ANSWER)

NEW QUESTION: 69

Which 0S1 model is used to insert an MPLS label?

A. between Layer 1 and Layer 2

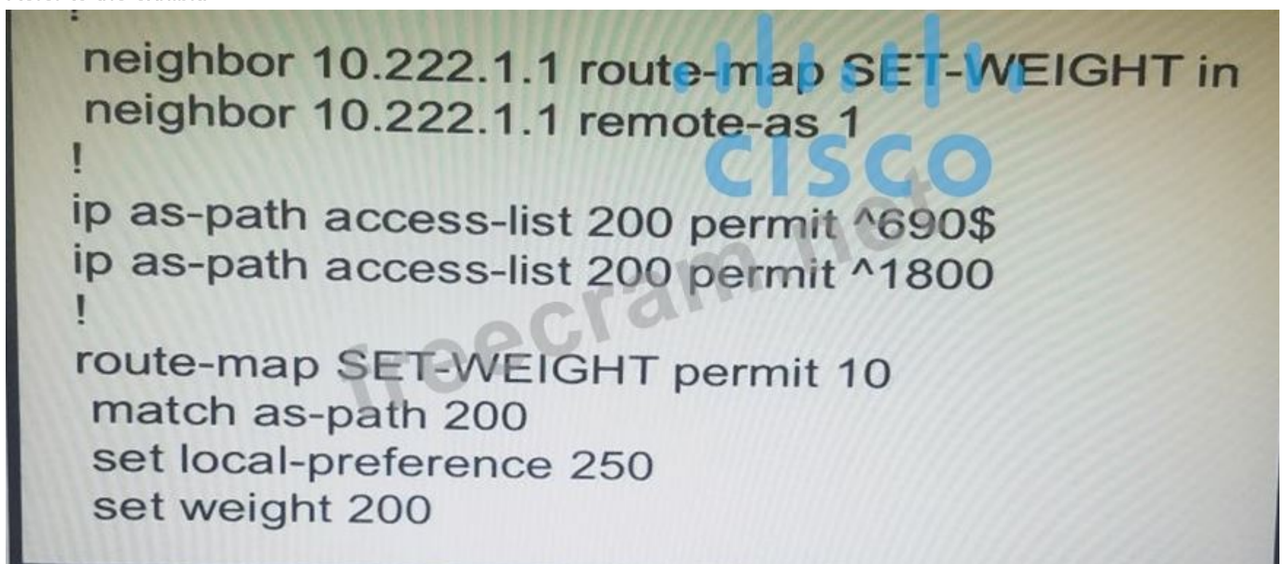
B. between Layer 5 and Layer 6

C. between Layer 2 and Layer 3

D. between Layer 3 and Layer 4

Answer: (SHOW ANSWER)

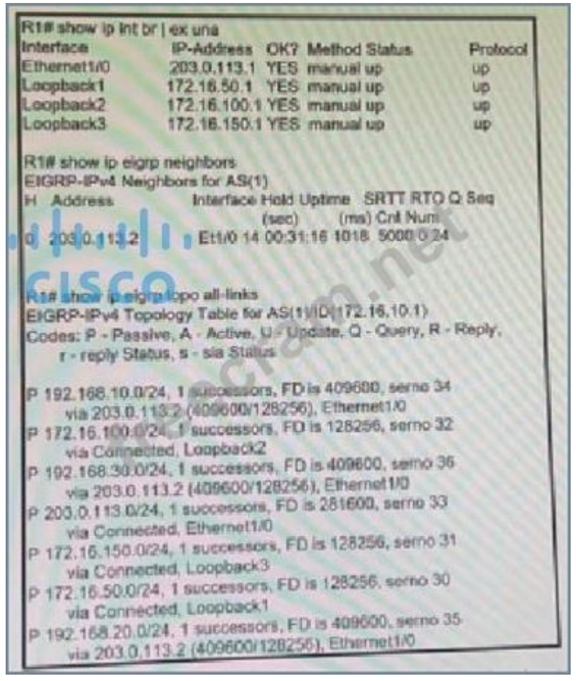
NEW QUESTION: 70
Refer to the exhibit.



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 10.222.1.1?
A. The weight value in another neighbor statement is higher than 200.
B. The route map is applied in the wrong direction.
C. The local preference value in another neighbor statement is higher than 250.
D. The local preference value should be set to the same value as the weight in the route map.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Which mechanism provides traffic segmentation within a DMVPN network?
A. RSVP
B. BGP
C. MPLS
D. iPsec
Answer: (SHOW ANSWER)
To use the DMPVN - Traffic Segmentation Within DMVPN feature you must configure Multiprotocol Label Switching (MPLS) by using the mpls ip command.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-dmvpn.html

NEW QUESTION: 72
Refer to the exhibit.



Routers R1 and R2 have established a network adjacency using EIGRP, and both routers are advertising subnets to its neighbor. After issuing the show ip EIGRP topology all-links command in R1, some prefixes are no showing R2 as a successor. Which action resolves the issue?

A. Resolve the incorrect metric on the link.

B. Rectify the incorrect router ID in R2.

C. Configure the network statement on the neighbor.

D. Enable split-horizon.

Answer: (SHOW ANSWER)

NEW QUESTION: 73

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.

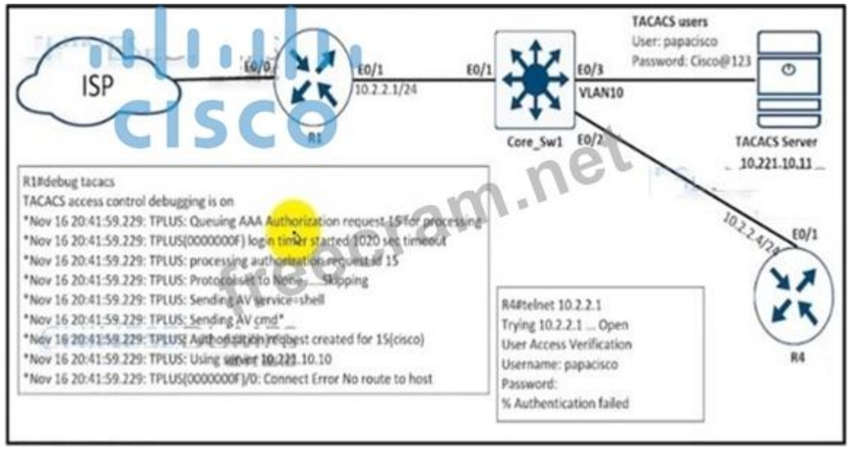
Answer: (SHOW ANSWER)

From the last line of the output, we notice that the result was "Invalid AUTHEN packet". Therefore something went wrong with the username or password.

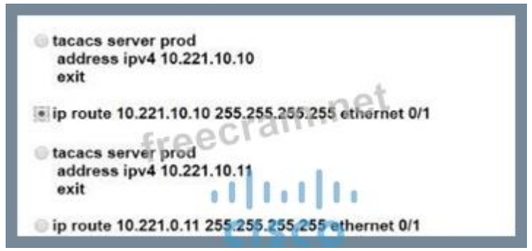
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access- control-system-tacacs-/200467-Troubleshoot-TACACS-Authentication-Issue.html

NEW QUESTION: 74

Refer to the exhibit.



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



A. Option C
B. Option B
C. Option A
D. Option D
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75

Refer to the exhibit An engineer must ensure that R3 sees only type 1 and 2 LSAs in area 1. Which command must the engineer apply on R2?
A. Area 1nssa no-summary
B. Area 1 stub nssa
C. Area 1 stub
D. Area a stub no-summary
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
Which function does LDP provide in an MPLS topology?
A. It enables a MPLS topology to connect multiple VPNs to P routers.
B. It provides hop-by-hop forwarding in an MPLS topology for LSRs.
C. It exchanges routes for MPLS VPNs across different VRFs.

D. It provides a means for LSRs to exchange IP routes.
Answer: (SHOW ANSWER)
LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4t/mp-ldp-12-4t-book.pdf

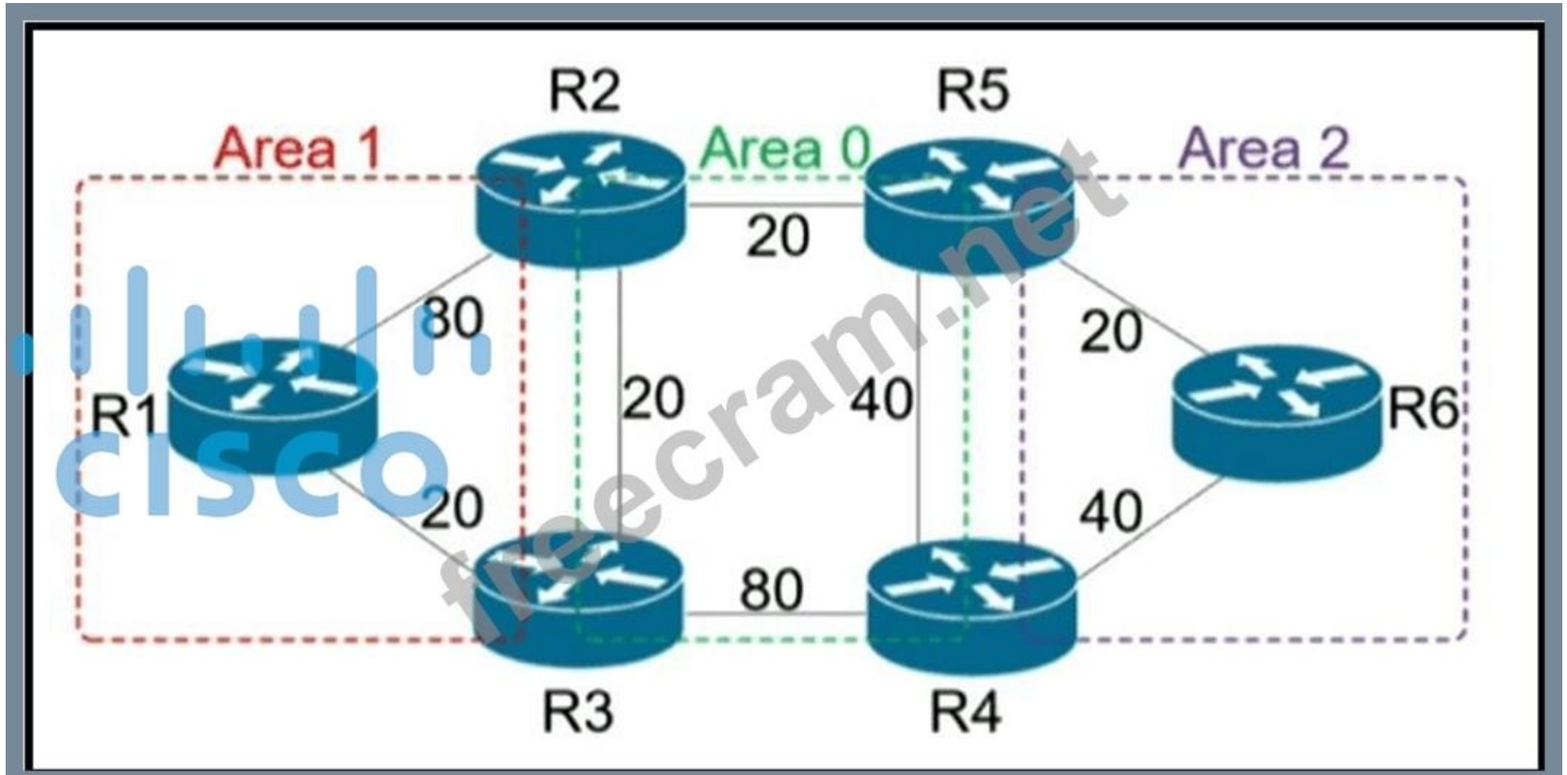
NEW QUESTION: 77
Which statement about route distinguishers in an MPLS network is true?
A. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
B. Route distinguishers are used for label bindings.
C. Route distinguishers make a unique VPNv4 address across the MPLS network.
D. Route distinguishers define which prefixes are imported and exported on the edge router.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html

NEW QUESTION: 79
Refer to the exhibit.



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

A. Increase the cost to 61 between R2 and R3

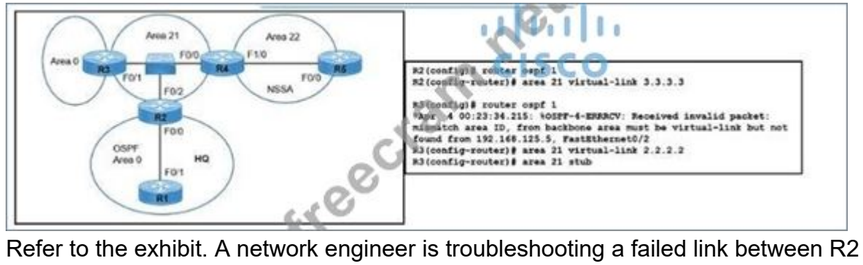
B. Increase the cost to 61 between R2-R3-R1

C. Decrease the cost to 2 between R6-R5-R2

D. Decrease the cost to 41 between R2 and R1

Answer: (SHOW ANSWER)

NEW QUESTION: 80



Refer to the exhibit. A network engineer is troubleshooting a failed link between R2 and R3 No traffic loss is reported from router R5 to HQ Which command fixes the separated backbone?

A. R2(config-router)#no area 21 stub

B. R2(config_router)#area 21 virtual-link 192.168.125.5

C. R3(config-router)#no area 21 stub

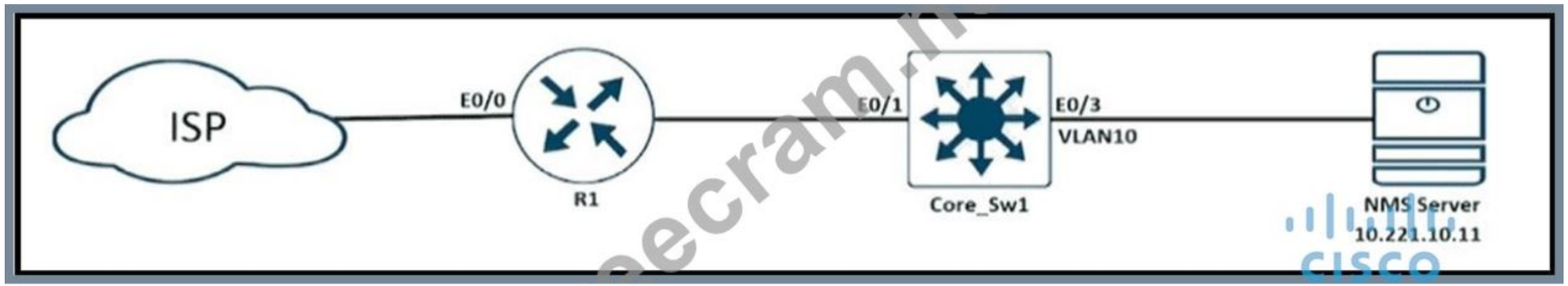
D. R3(config-router)#area 21 virtual-link 192.168.125.5
Answer: (SHOW ANSWER)

NEW QUESTION: 81
How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?
A. by address family
B. byRT
C. by RD
D. by MP-BGP
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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 \ the command is entered, it gets rejected. Which command set is used to troubleshoot and reserve this issue?
A. line con 0aaa authorization consoleauthorization exec!line vty 0 4transport input ssh
B. line con 0aaa authorization consoleauthorization priv15!line vty 0 4transport input ssh
C. line con 0aaa authorization console priv15!line vty 0 4authorization exec
D. line con 0aaa authorization console!line vty 0 4authorization exec
Answer: (SHOW ANSWER)
NEW QUESTION: 83
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. no snmp trap link-status

B. snmp trap ip verify drop-rate

C. snmp trap link-status down

D. ip verify drop-rate notify hold-down 60

Answer: (SHOW ANSWER)

NEW QUESTION: 84

```
admin@linux:~$ telnet 198.51.100.64
Trying 198.51.100.64...
Connected to 198.51.100.64.
Escape character is '^]'.

User Access Verification

Password: admin
CPE> exit
Connection closed by foreign host.
admin@linux:~$ ssh 198.51.100.64
admin@198.51.100.64's password: admin
Permission denied, please try again.
admin@198.51.100.64's password: admin
Permission denied, please try again.
admin@198.51.100.64's password: admin
Connection closed by 198.51.100.64 port 22
admin@linux:~$
```

Refer to the exhibit. An administrator can log in to the device using Telnet but the attempts to log in to the same device using SSH with the same credentials fail Which action resolves this issue?

A. Configure transport input all on the VTY lines to allow SSH

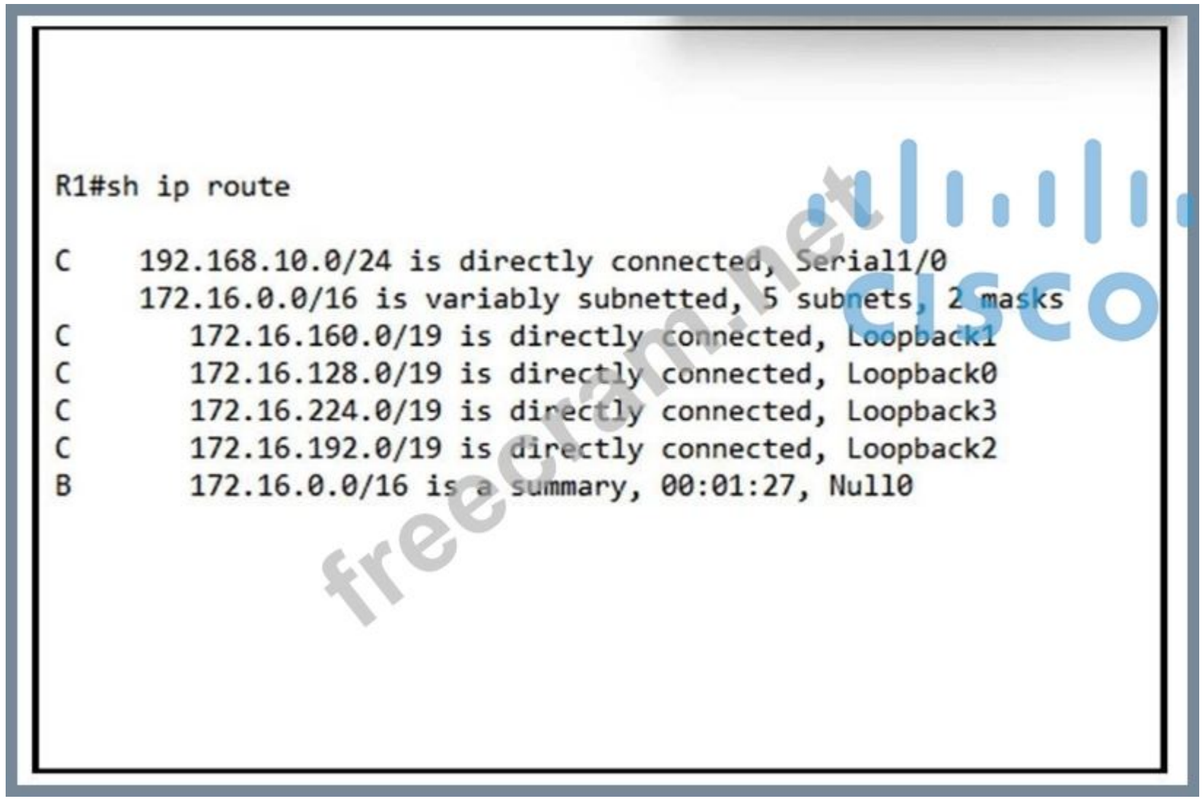
B. Configure SSH service on the router

C. Configure to use the Telnet user database for SSH as well
D. Configure the VTY lines with login local
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Which two protocols are used by a P router to transfer VPN traffic between PE routers in an MPLS network?
(Choose two.)
A. BGP
B. RSVP
C. OSPF
D. LDP
E. MP-BGP
Answer: (SHOW ANSWER)

NEW QUESTION: 86
A newly Installeo router starts establishing an LDP session from another MPLS router to which it is not directly connected. Which LDP message type responds by target router to the Initiating router using UDP protocol?
A. advertisement message
B. notification message
C. session message
D. extended discovery message
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87



Refer to the exhibit. Which configuration advertises more specific routes to R1 without sending a BGP summary route?

A. R1#configure terminal
R1 (config)#router BGP 100
R1 (config-router)#auto-summary

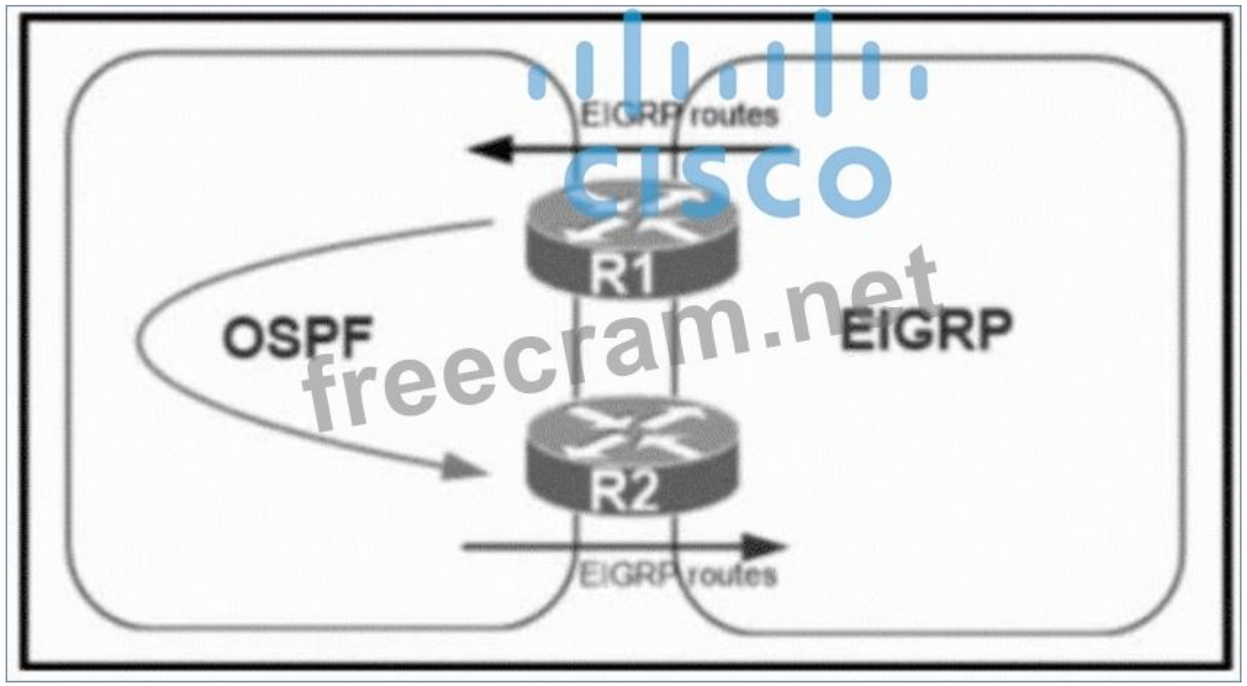
B. R1#configure terminal
R1 (config)#rouler BGP 100
R1 (conflg-router)#no auto-summary

C. R2#configure terminal
R2 (conflg)#router BGP 100
R2 (config-rouler)#no auto-summary

D. R2#configure terminal
R2 (config)#router BGP 100
R2 (config-router)#auto-summary

Answer: (SHOW ANSWER)

NEW QUESTION: 88



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 deny 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 allow when redistributing OSPF into EIGRP.

C. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.

D. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.

Answer: (SHOW ANSWER)

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
```

NEW QUESTION: 89

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 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 MTU settings on both routers.

C. Configure to match the OSPF interface unique IP address and subnet mask on both routers.

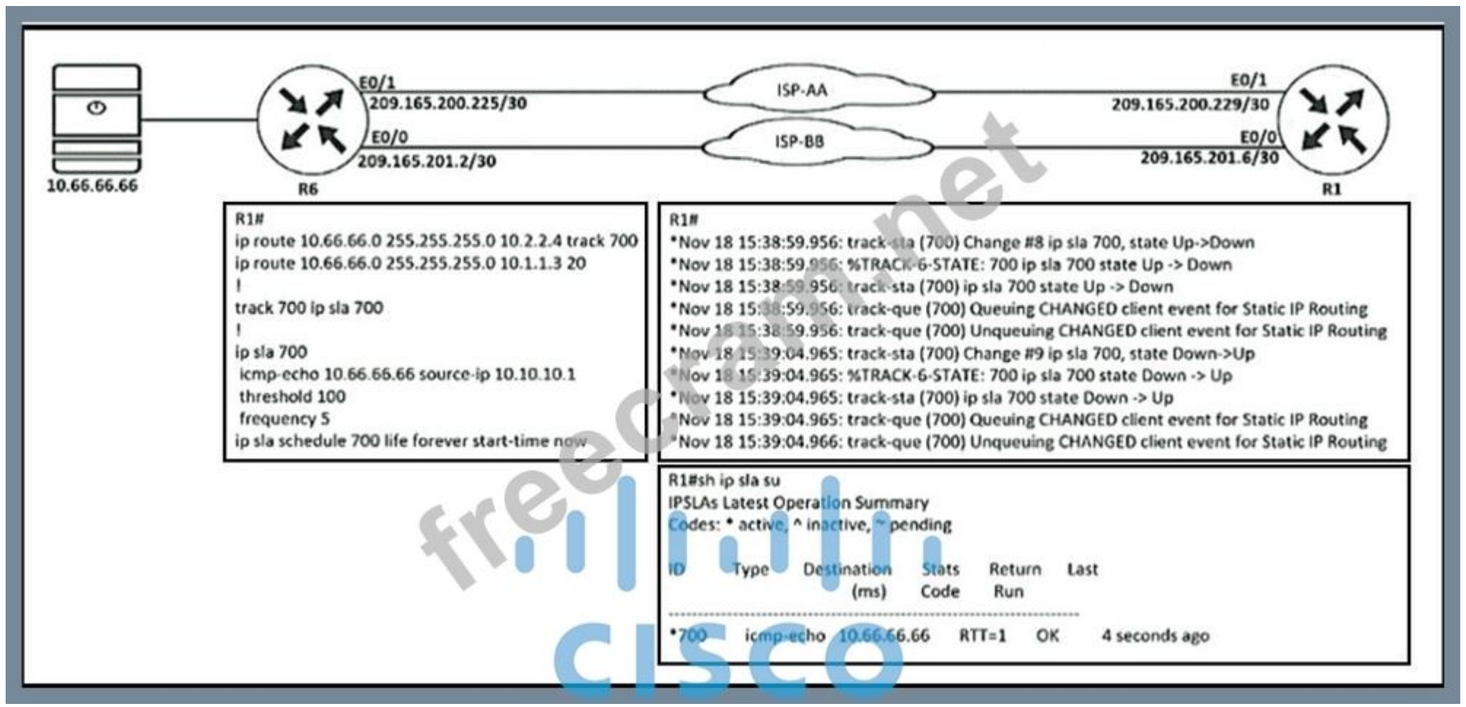
D. Configure to match the OSPF interface network types on both routers.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 90

Refer to the exhibit.



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

NEW QUESTION: 91

Refer to the exhibit. Which action resolves the issue?

A. Establish connectivity between the NTP server and the switch.

B. Configure the local time on the SW1 device

C. Configure the local time on Cisco DNA Center

D. Establish connectivity between the NTP server and Cisco DNA Center.

Answer: (SHOW ANSWER)

NEW QUESTION: 92

Refer to the exhibit.

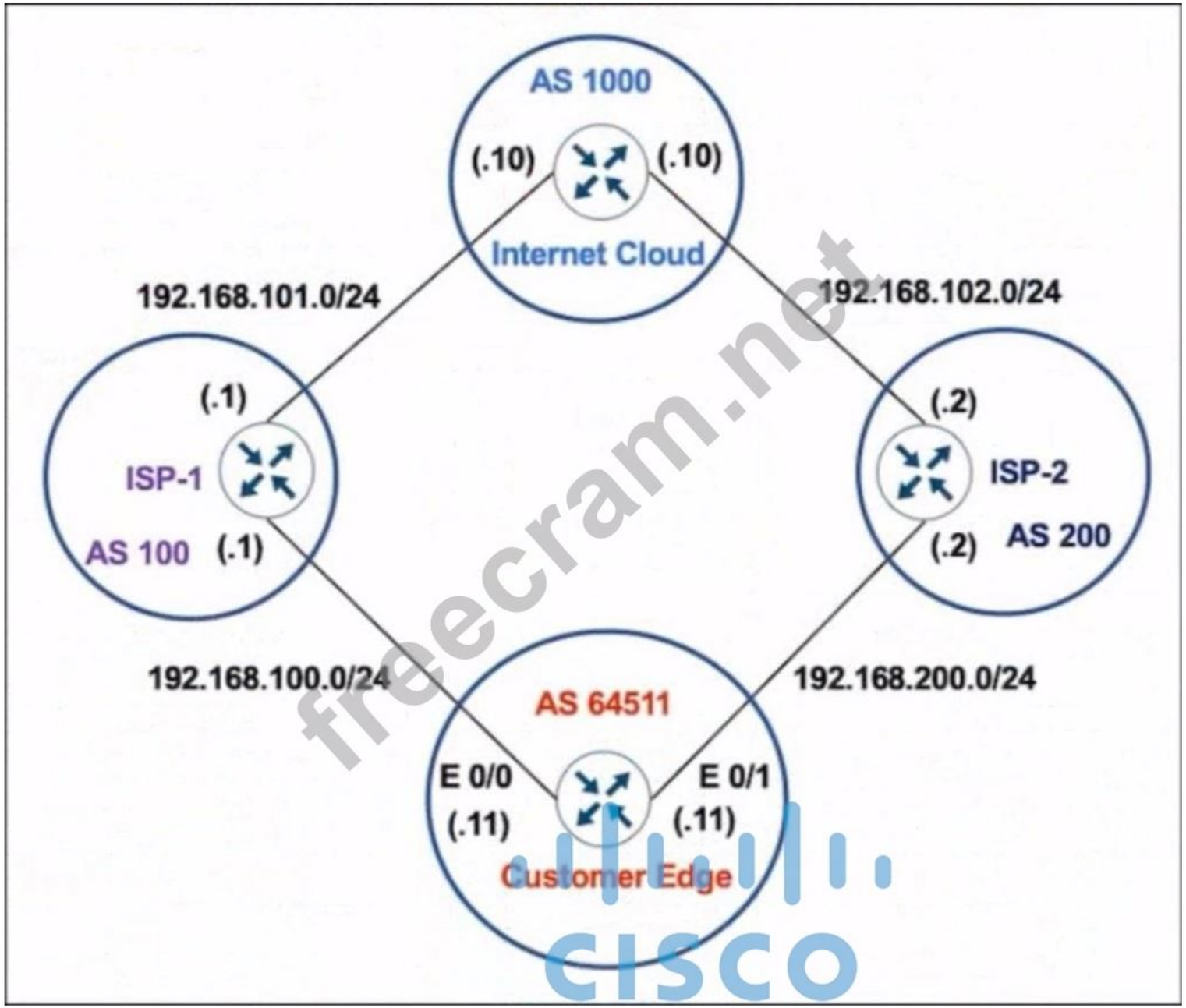
```
snmp-server community ciscotest1
snmp-server host 192.168.1.128 ciscotest
snmp-sever enable traps bgp
```

Network operations cannot read or write any configuration on the device with this configuration from the operations subnet. Which two configurations fix the issue? (Choose two.)

A. Modify access list 1 and allow SNMP in the access list.

B. Configure SNMP rw permission in addition to version 1.
C. Configure SNMP rw permission in addition to community ciscotest 1.
D. Configure SNMP rw permission in addition to community ciscotest.
E. Modify access list 1 and allow operations subnet in the access list.
Answer: (SHOW ANSWER)

NEW QUESTION: 93



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 64511aggregate-address 172.16.20.0 255.255.252.0 summary-only
B. router bgp 64511neighbor 192.168.100.1 summary-onlyneighbor 192.168.200.2 summary-only
C. interface E 0/0ip bgp suppress-map BLOCK_SPECIFIC!interface E 0/1ip bgp suppress-map BLOCK_SPECIFIC!ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22 ge 24!route-map BLOCK_SPECIFIC permit 10match ip address prefix-list PL_BLOCK_SPECIFIC
D. ip prefix-list PL_BLOCK_SPECIFIC deny 172.16.20.0/22 ge 22ip prefix-list PL BLOCK SPECIFIC permit 172.16.20.0/22!route-map BLOCK_SPECIFIC permit 10match ip address prefix-list PL_BLOCK_SPECIFIC!router bgp 64511aggregate-address 172.16.20.0 255 255.252.0 suppress-map BLOCKSPECIFIC
Answer: (SHOW ANSWER)
When the aggregate-address command is used within BGP routing, the aggregated address is advertised, along with the more specific routes. The exception to this rule is through the use of the summary-only command. The "summary-only" keyword suppresses the more specific routes and announces only the summarized route.

NEW QUESTION: 94
Refer to Exhibit.

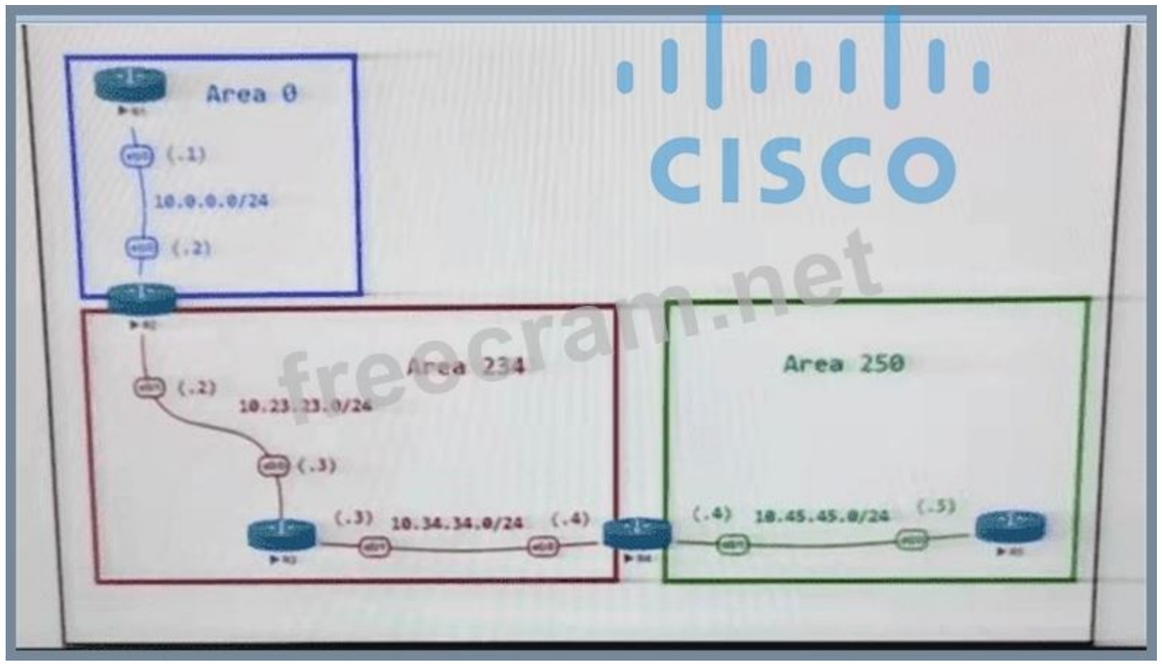
A network administrator added one router in the Cisco DNA Center and checked its discovery and health from the Network Health Dashboard. The network administrator observed that the router is still showing up as unmonitored.
What must be configured on the router to mount it in the Cisco DNA Center?
A.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

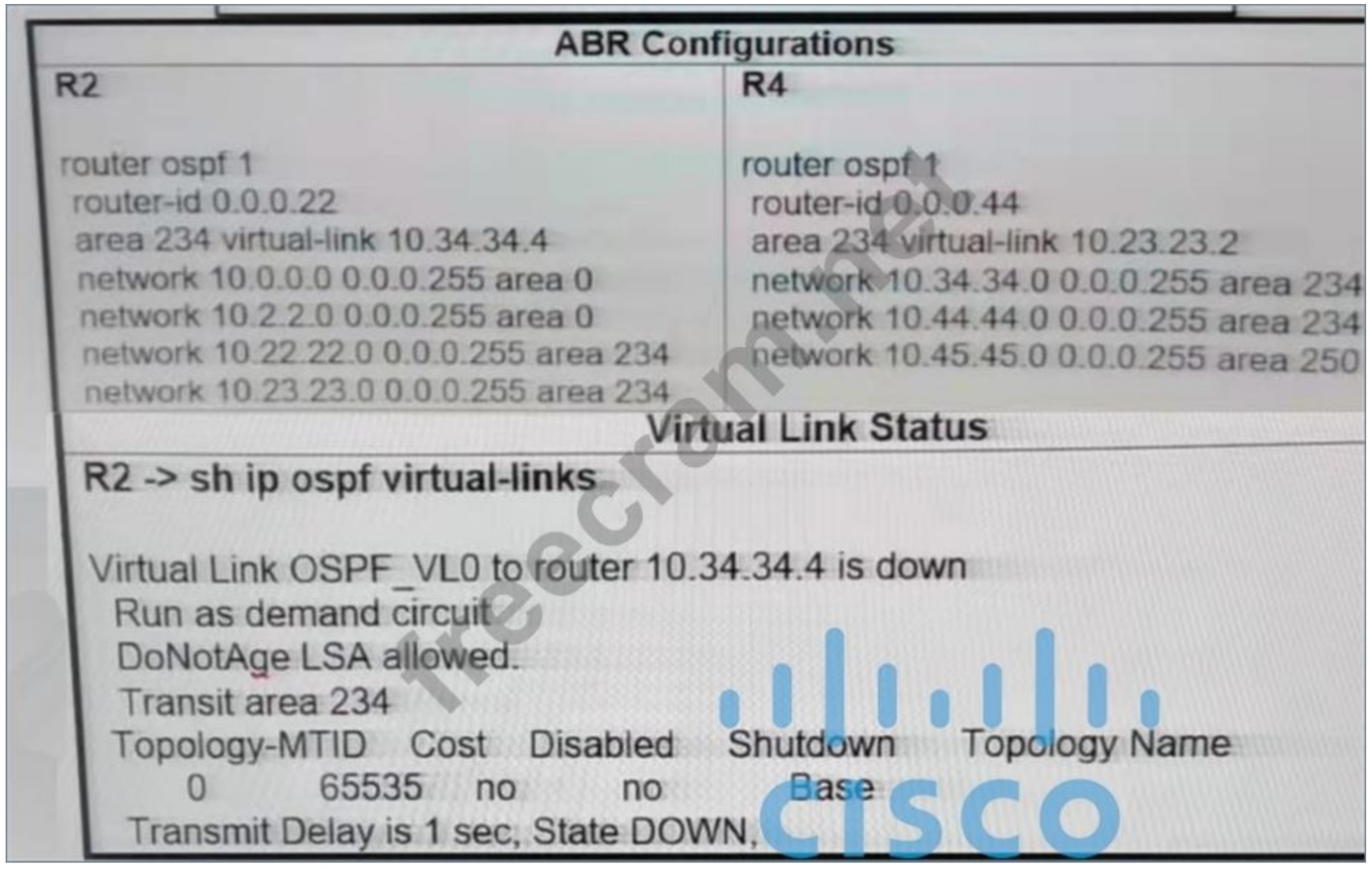
D. Configure router with SNMPv2c or SNMPv3 traps
Answer: (SHOW ANSWER)
Unmonitored: Unmonitored devices are devices for which Assurance did not receive any telemetry data during the specified time range.

NEW QUESTION: 95
:586
While BGP internet routes are redistributed to a lower class of router via RIP. packets are being dropped and routes are failing to be distributed in RIP. Which action resolves the issue?
A. Use OSPF instead of RIP to accept all BGP routes.
B. Use RIP V2 to be able to use classless networks from BGP
C. Use the input-queue command to prevent the loss of packets.
D. Use WFQ in the output queue of the high-performance router.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
What statement about route distinguishes in an MPLS network is true?
A. Route distinguishes define which prefixes are imported and exported on the edge router
B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
C. Route distinguishes make a unique VPNv4 address across the MPLS network.
D. Route distinguishes are used for label bindings
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
Refer to the exhibit.





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

A. R2router ospf 1router-id 10.23.23.2

B. R2router ospf 1no area area 234 virtual-link 10.34.34.4area 0 virtual-link 0.0.0.44

C. R4router ospf 1no area 234 virtual-link 10.23.23.2area 234 virtual-link 0.0.0.22

D. R2router ospf 1no area 234 virtual-link 10.34.34.4area 234 virtual-link 0.0.0.44

E. R4router ospf 1no area area 234 virtual-link 10.23.23.2area 0 virtual-link 0.0.0.22

Answer: (SHOW ANSWER)

Reference: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html An important thing to remember when configuring virtual-link is we need to configure the OSPF router ID and NOT the IP address of the ABR. Therefore in this question we have to use the command "area
234 virtual-link 0.0.0.44" on R2 and "area 234 virtual-link 0.0.0.22" on R4.

NEW QUESTION: 98

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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-snooping.pdf

NEW QUESTION: 99

```
R3#show cef interface gi0/3
GigabitEthernet0/3 is up (if_number 5)
  Corresponding hwidb fast_if_number 5
  Corresponding hwidb firstsw->if_number 5
  Internet address is 172.16.4.253/30
  ICMP redirects are never sent
  Per packet load-sharing is disabled
  IP unicast RPF check is enabled
  Input features: uRPF
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is GigabitEthernet0/3
  Fast switching type 1, interface type 27
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
  Input fast flags 0x4000, Output fast flags 0x0
  ifindex 5(5)
  Slot  Slot unit 7 VC -1
  IP MTU 1500
R3#show run int gi0/3
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet0/3
 ip address 172.16.4.253 255.255.255.252
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
end
```

Refer to the exhibit. An engineer implements uRPF to increase security and stop incoming spoofed IP packets. Some asymmetrically routed packets are also blocked after the configuration. Which command resolves the issue?
A. ip verify unicast reverse-path any
B. ip verify unicast source reachable-via any
C. ip verify unicast source reachable-via rx
D. ip verify unicast reverse-path
Answer: B (LEAVE A REPLY)

NEW QUESTION: 100
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
```

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?
A. access-class INTERNET in

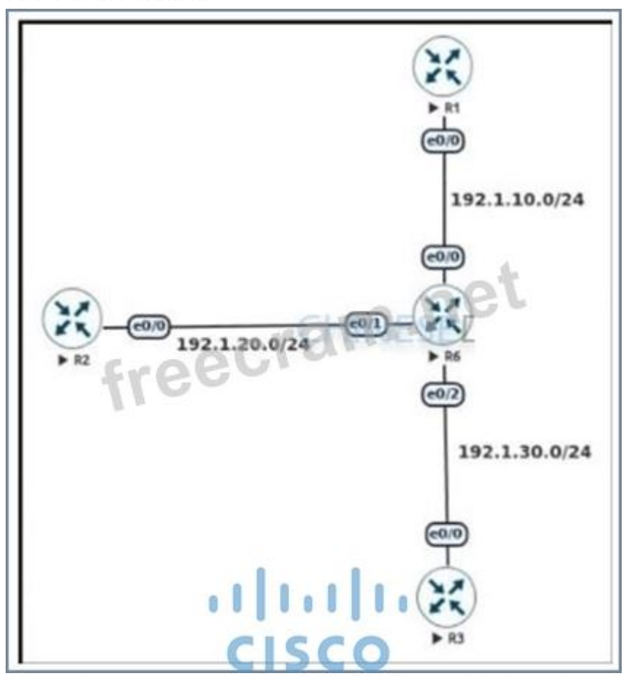
B. ipv6 access-class INTERNET in
C. ipv6 traffic-filter INTERNET in
D. ip access-group INTERNET in
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Refer to the exhibit.

```
RtrA#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(1)/ID(10.1.6.1)
.....snip.....
P 10.200.1.0/24, 1 successors, FD is 21026560
via 10.1.1.2 (21026560/20514560), Serial1/0
via 10.1.2.2 (46740736/20514560), Serial1/1
via 10.1.3.2 (46740736/46228736), Serial1/2
```

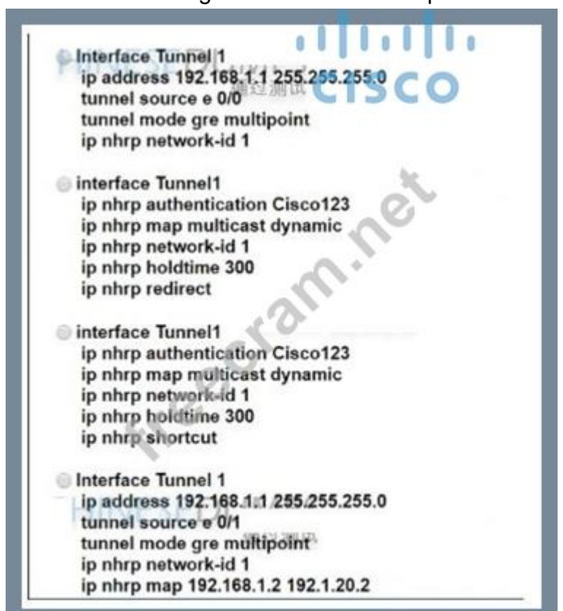
Which action makes 10.1.3.2 the feasible successor to reach 10. 200. 1 0/24 for location S42T447E33F95?
A. Increase path bandwidth higher than 1011 2 and lower than 1012 2 between RtrA and the destination
B. Increase path bandwidth higher than 10.1 2 2 and higher than 10.1.1.2 between RtrA and the destination
C. Increase path bandwidth higher than 10.1 2 2 and lower than 101.1.2 between RtrA and the destination.
D. Increase path bandwidth lower than 1011 2 and lower than 1012 2 between RtrA and the destination
Answer: (SHOW ANSWER)

NEW QUESTION: 102
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. Option D
B. Option A
C. Option C
D. Option B
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
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: (SHOW ANSWER)

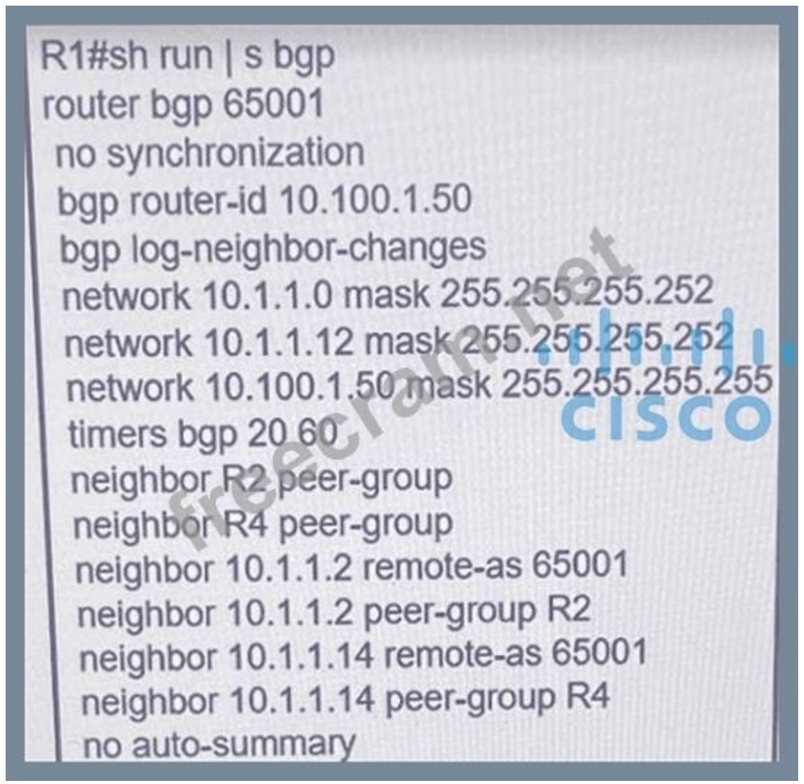
The **set ip default next-hop** command verifies the existence of the destination IP address in the routing table, and...

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

NEW QUESTION: 104
What is the purpose of the DHCPv6 Guard?
A. It messages between a DHCPv6 server and a DHCPv6 client (or relay agent).
B. It shows that clients of a DHCPv5 server are affected.
C. It block DHCPv6 messages from relay agents to a DHCPv6 server.

D. It allows DHCPv6 replay and advertisements from (rouge) DHCPv6 servers.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6fxe-16-book/ip6-dhcpv6-guard.html

NEW QUESTION: 105
Refer to the exhibit.



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 10.1.1.2 route-reflector-client
B. neighbor 10.1.1.2 allowas-in
C. neighbor R2 route-reflector-client
D. neighbor 10.1.1.14 route-reflector-client
E. neighbor R4 route-reflector-client
Answer: (SHOW ANSWER)

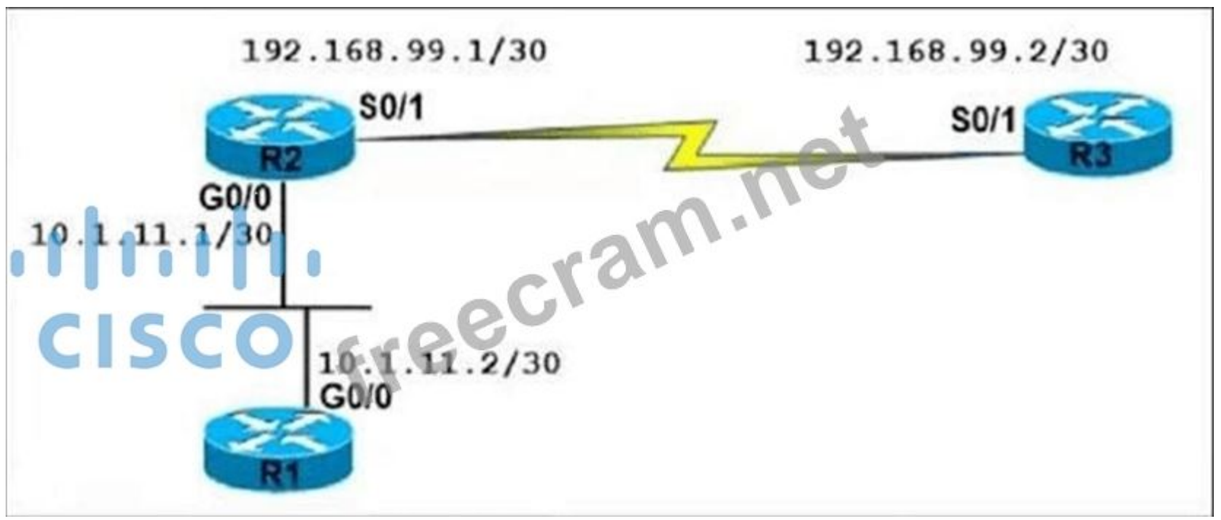
NEW QUESTION: 106
Which protocol is used in a DMVPN network to map physical IP addresses to logical IP addresses?
A. BGP
B. LLDP

C. EIGRP
D. NHRP
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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 a user on the source router with the username tftp password tftp command
B. Copy the file to the destination router with the copy tftp: flash: command
C. TFTP is not supported in recent IOS versions, so an alternative method must be used
D. Configure the TFTP authentication on the source router with the tftp-server authentication local command
E. Enable the TFTP server on the source router with the tftp-server flash: <filename> command
Answer: (SHOW ANSWER)

NEW QUESTION: 108
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
192.168.99.1      1   EXSTART/        00:00:33    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. Restore the Layer 2/Layer 3 conectivity issue in the ISP network.

B. Match MTU on both router interfaces or ignore MTU.

C. Administrative "shut then no shut" both router interfaces.

D. Enable OSPF on the interface, which is required.

Answer: B (LEAVE A REPLY)

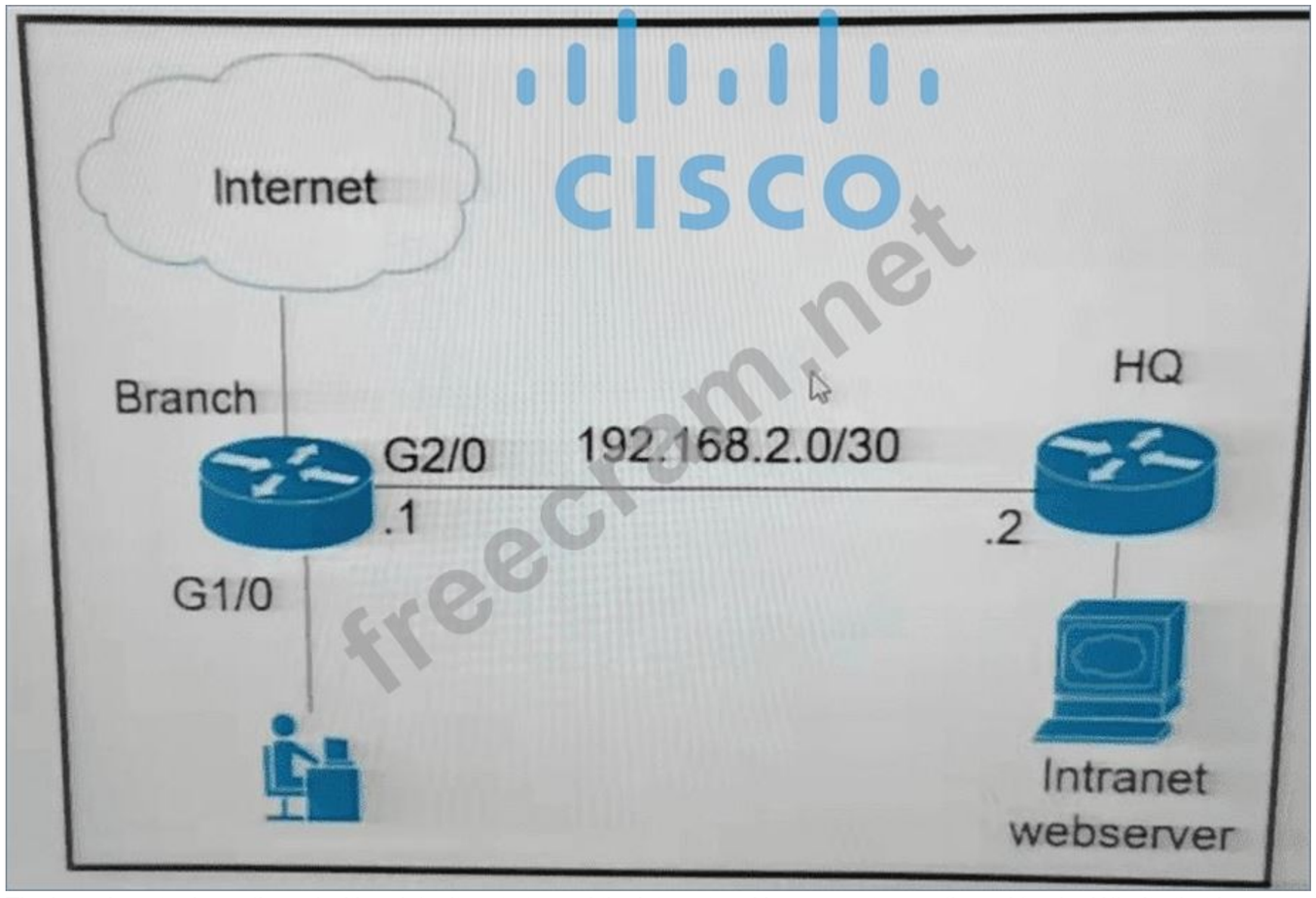
After two OSPF neighboring routers establish bi-directional communication and complete DR/BDR election (on multi-access networks), the routers transition to the exstart state. In this state, the neighboring routers establish a master/slave relationship and determine the initial database descriptor (DBD) 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 that the MTU set on the neighboring router, the neighboring router ignores the packet.

NEW QUESTION: 109

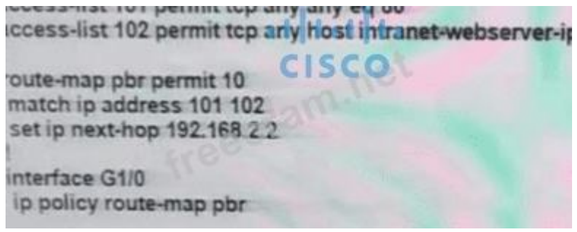
Refer to the exhibit.

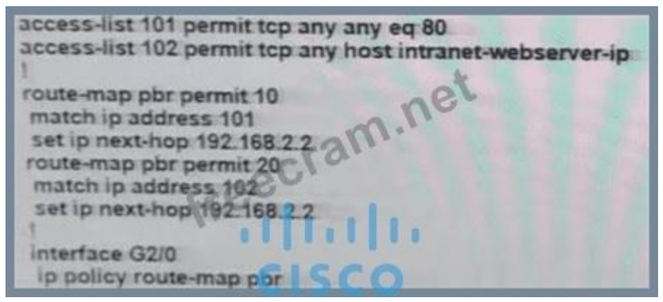


The branch router is configured with a default route toward the internet and has no routes configured for the HQ site that is connected through interface G2/0. The HQ router is fully configured and does not require changes. Which configuration on the branch router makes the intranet website (TCP port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

A.

```
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
```

B.


C.


D.


Answer: (SHOW ANSWER)

the ACL 101 matches all HTTP pakects while the ACL 102 matches TCP packets destined to Intranet webserver. These packets will be sent to HQ router.

If a match command refers to several objects in one command, either of them should match (the logical OR algorithm is applied). For example, in the match ip address 101 102 command, a route is permitted if it is permitted by access list 101 or access list 102.

NEW QUESTION: 110

Refer to the exhibit.

Router Configuration:

```
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-adjacency-changes
 !
router ospf 2 vrf customer_a
 log-adjacency-changes
 network 192.168.4.0 0.0.0.255 area 0
 !
end
```

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 1:2
 route-target import 1:2
```

```
ip vrf customer_a
 rd 1:1
 route-target import 1:1
 route-target export 1:2
```

```
ip vrf customer_a
 rd 1:2
 route-target both 1:2
```

```
ip vrf customer_a
 rd 1:2
 route-target both 1:1
```

A. Option A

B. Option B

C. Option C

D. Option D

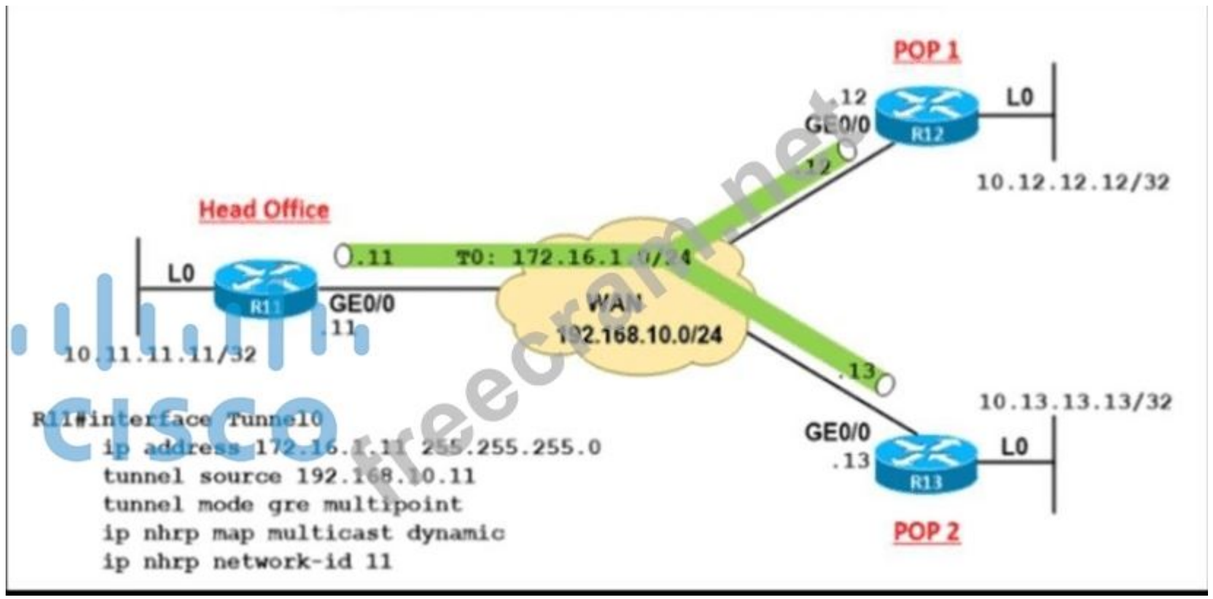
Answer: (SHOW ANSWER)

From the exhibit, we learned:

+ VRF customer_a was exported with Route target (RT) of 1:1 so at the remote site it must be imported with the same RT 1:1.

+ VRF customer_a was imported with Route target (RT) of 1:1 so at the remote site it must be exported with the same RT 1:1.
Therefore at the remote site we must configure the command "route-target both 1:1" (which is equivalent to two commands "route-target import 1:1" & "route-target export 1:1".

NEW QUESTION: 111



Refer to the exhibit A company builds WAN infrastructure between the head office and POPs using DMVPN hub-and-spoke topology to provide end-to-end communication All POPs must maintain point-to-point connectivity with the head office Which configuration meets the requirement at routers R12 and R13?

○ R12#
interface Tunnel0
ip nhrp map multicast 192.168.10.11
ip nhrp map 172.16.1.11 192.168.10.11
ip nhrp network-id 12
ip nhrp nhs 172.16.1.11

R13#
interface Tunnel0
ip nhrp map multicast 192.168.10.11
ip nhrp map 172.16.1.11 192.168.10.11
ip nhrp network-id 13
ip nhrp nhs 172.16.1.11

○ R12#
interface Tunnel0
ip nhrp map multicast 172.16.1.11
ip nhrp map 172.16.1.11 192.168.10.11
ip nhrp network-id 12
ip nhrp nhs 192.168.10.11

R13#
interface Tunnel0
ip nhrp map multicast 172.16.1.11
ip nhrp map 172.16.1.11 192.168.10.11
ip nhrp network-id 13
ip nhrp nhs 192.168.10.11

Configure routers R12 and R13 as:

```
interface Tunnel0
 ip nhrp map multicast 172.16.1.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 11
 ip nhrp nhs 192.168.10.11
```

Configure routers R12 and R13 as:

```
interface Tunnel0
 ip nhrp map multicast 192.168.10.11
 ip nhrp map 172.16.1.11 192.168.10.11
 ip nhrp network-id 11
 ip nhrp nhs 172.16.1.11
```


A. Option C
B. Option A
C. Option D
D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 112
How are CE advertised routes segmented from other CE routers on an MPLS PE router?
A. with a combination of VRF-Lite and MP-BGP
B. by pushing MPLS labels advertised by LDP on customer routes
C. by enabling multiple instances of BGP. one for each CE router
D. by assigning CE-facing interfaces to different VRFs
Answer: (SHOW ANSWER)
In an MPLS PE router, CE advertised routes are segmented from other CE routers by assigning CE-facing interfaces to different Virtual Routing and Forwarding (VRF) instances12. A VRF is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. By associating a network interface with a VRF, the network layer (Layer 3) has a different view of the network topology. This allows the segmentation of routing paths for traffic from different customers or different types of traffic. In the context of MPLS, VRFs are used to create separate routing instances for each customer on a PE router3.
References:
Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) training videos CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide Implementing Cisco Enterprise Advanced Routing and Services source documents or study guide MPLS routes to advertise from CE to PE - Cisco Community Configuring Route Exchange Between PE and CE Devices - CloudEngine 12800 and 12800E V200R005C10 Configuration Guide - VPN - Huawei Customer edge router - Wikipedia

NEW QUESTION: 113
Which two methods use IPsec to provide secure connectivity from the branch office to the headquarters office? (Choose two.)

A. PPPoE
B. DMVPN
C. Virtual Tunnel Interface (VTI)
D. MPLS VPN
E. SSL VPN
Answer: (SHOW ANSWER)

NEW QUESTION: 114
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: (SHOW ANSWER)
To ACL should be permit tcp 101 10.1.1.1 0.0.0.0

NEW QUESTION: 115

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?

A. Enter the service timestamps log datetime localtime 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 clock-period global command

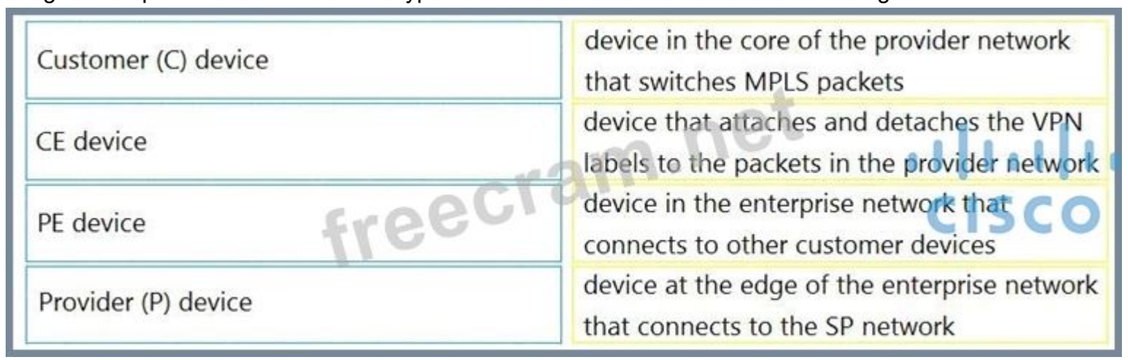
Answer: (SHOW ANSWER)

If a router is configured to get the time from a Network Time Protocol (NTP) server, the times in the router's log entries may be different from the time on the systemclock if the [localtime] option is not in the service timestamps log command. To solve this issue, add the [localtime] option to the service timestamps log command. Thetimes should now be synchronized between the system clock and the log message timestamps.
Reference: https://community.cisco.com/t5/networking-documents/router-log-timestamp-entries-are-different- from-the-system-clock/ta-p/3132258

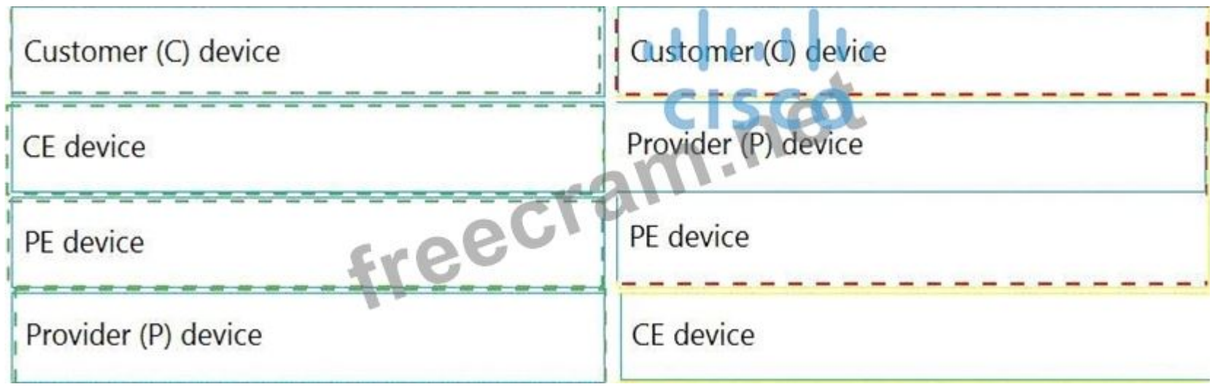
NEW QUESTION: 116
What are the two benefits of using BFD? (Choose two.)
A. subsecond failure detection
B. forwarding path failure detection

C. synchronous path determination
D. supports UDL failure
E. supports all routing protocols
Answer: (SHOW ANSWER)

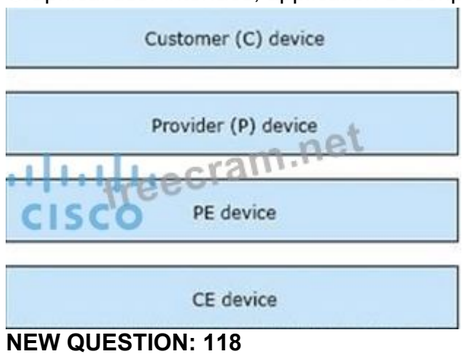
NEW QUESTION: 117
Drag and drop the MPLS VPN device types from the left onto the definitions on the right.



Answer:



Explanation:
Graphical user interface, application Description automatically generated



NEW QUESTION: 118

Refer to the exhibit.

```
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
```

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

A. NYrouter ospf 1area 0 authentication message-digest

B. LAinterface E 0/0ip ospf message-digest-key 1 md5 Cisco123

C. NYinterface E 0/0no ip ospf message-digest-key 1 md5 Cisco123ip ospf authentication-key Cisco123

D. LAinterface E 0/0ip ospf authentication-key Cisco123

E. LArouter ospf 1area 0 authentication message-digest

Answer: (SHOW ANSWER)

The configuration on NY router is good for OSPF authentication. So we must enable OSPF authentication on LA router with the following commands:

router ospf 1

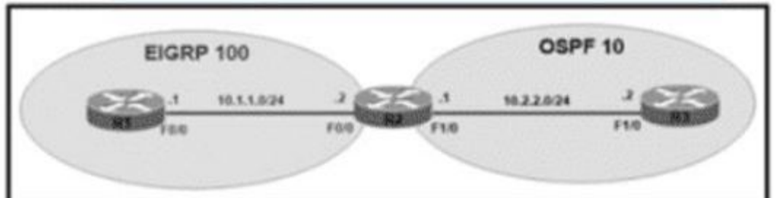
area 0 authentication message-digest

interface E0/0

ip ospf message-digest-key 1 md5 Cisco123

NEW QUESTION: 119

:590



R1 Configuration:
interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
!
router eigrp 100
network 10.0.0.0

R2 Configuration:
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
!
interface FastEthernet1/0
ip address 10.2.2.1 255.255.255.0
!
router eigrp 100
network 10.0.0.0
!
router ospf 1
network 10.2.2.1 0.0.0.0 area 0
!

R1 Routing Table Output:
R1#sh ip route
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/24 is directly connected, FastEthernet0/0
L 10.1.1.1/32 is directly connected, FastEthernet0/0
D 10.2.2.0/24 [90/30720] via 10.1.1.2, 01:19:35, FastEthernet0/0

Refer to the exhibit The R2 OSPF route 10 2 2 0/24 shows in the R1 EIGRP routing table without route redistribution performed between OSPF and EIGRP routing protocols Which configuration is required on router R2 to resolve the issue?

A. Replace the network 10.0.0.0 command with FastEthernet0/0network in EIGRP 100.
B. passive-interface FastEthernet 0/0 command in OSPF1.
C. Addthe passive-interface FastEthernet 1/0 command in EIGRP 100
D. Add the no auto-summary command in EIGRP 100.
Answer: (SHOW ANSWER)

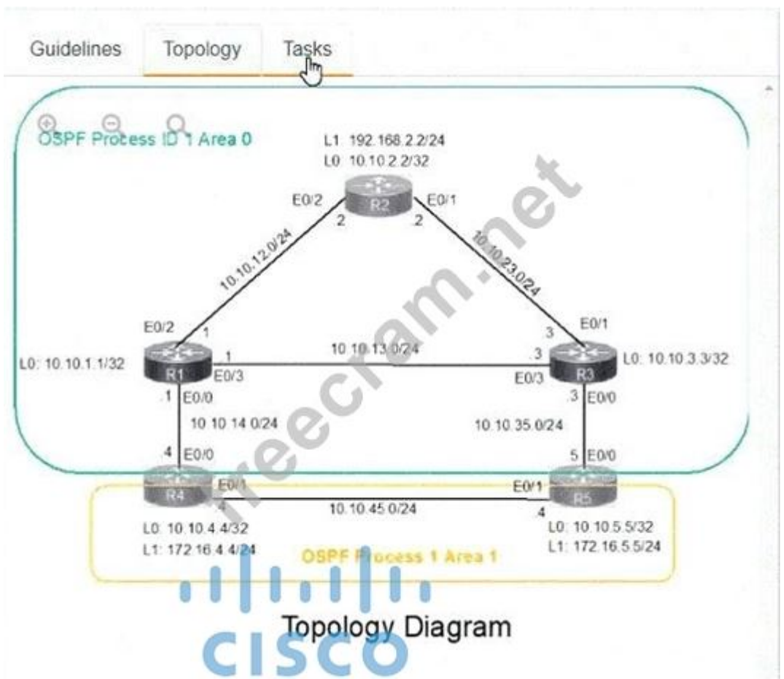
NEW QUESTION: 120
A network administrator is troubleshooting a failed AAA login issue on a Cisco Catalyst c3560 switch. When the network administrator tries to log in with SSH using TACACS+ username and password credentials, the switch is no longer authenticating and is failing back to the local account. Which action resolves this issue?

A. Configure ip tacacs-server source-interface GigabitEthernet 1/1
B. Configure ip tacacs source-interface GigabitEthernet 1/1
C. Configure ip tacacs source-ip 192.168.100.55

D. Configure ip tacacs-server source-ip 192.168.100.55
Answer: (SHOW ANSWER)

NEW QUESTION: 121
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. FlexVPN
B. GETVPN
C. Cisco Easy VPN
D. DMVPN
Answer: (SHOW ANSWER)

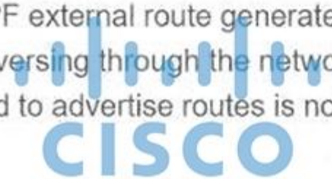
NEW QUESTION: 122
A network is configured with IP connectivity, and the routing protocol between devices started having problems right after the maintenance window to implement network changes. Troubleshoot and resolve to a fully functional network to ensure that:



Guidelines Topology Tasks

A network is configured with IP connectivity, and the routing protocol between devices started having problems right after the maintenance window to implement network changes. Troubleshoot and resolve to a fully functional network to ensure that:

1. Inter-area links have link authentication (not area authentication) using MD5 with the key 1 string CCNP.
2. R3 is a DR regardless of R2 status while R1 and R2 establish a DR/BDR relationship.
3. OSPF uses the default cost on all interfaces. Network reachability must follow OSPF default behavior for traffic within an area over intra-area VS inter-area links.
4. The OSPF external route generated on R4 adds link cost when traversing through the network to reach R2. A network command to advertise routes is not allowed.



R2 R4 R5

```
R2>en
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#sh run
Building configuration...
Current configuration : 1279 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
```

R2 R4 R5

```
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
 ip ospf 1 area 0
!
interface Loopback1
 ip address 192.168.2.2 255.255.255.0
 ip ospf 1 area 0
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.23.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/2
 ip address 10.10.12.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router ospf 1
 passive-interface default
 no passive-interface Ethernet0/1
 no passive-interface Ethernet0/2
```


R2 R4 R5

```
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router ospf 1
 passive-interface default
 no passive-interface Ethernet0/1
 no passive-interface Ethernet0/2
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
```


R4

R2 R4 R5

```
R4>
R4>
R4>
R4>
R4>en
R4#sh run
Building configuration...

Current configuration : 1479 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
 --More--
```

R2 R4 R5

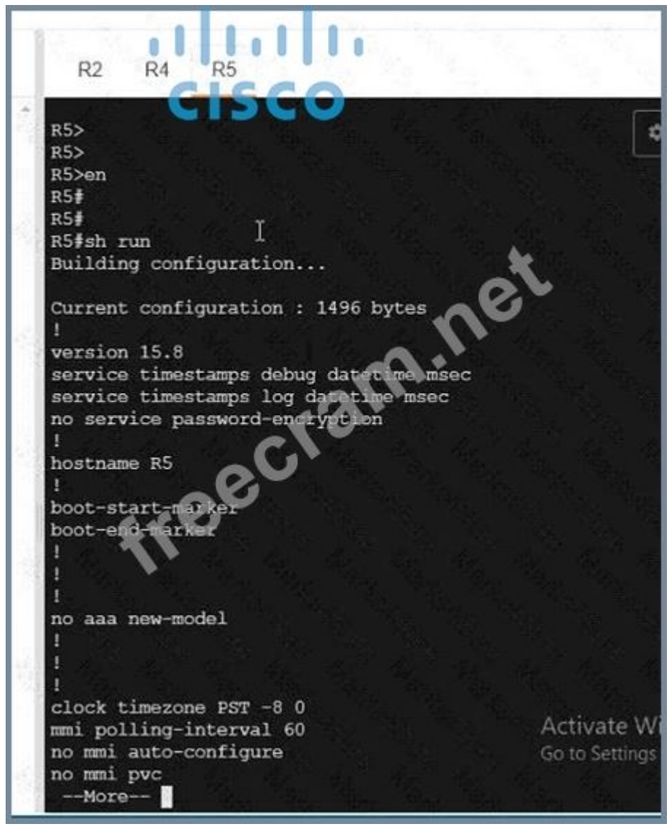
```
key chain CCNP
 key 1
  key-string ccnp
  cryptographic-algorithm md5
!
!
!
!
!
!
 ip address 172.16.4.4 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.14.4 255.255.255.0
 ip ospf authentication key-chain CCNP
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/1
 ip address 172.16.45.4 255.255.255.0
 ip ospf 1 area 1
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
```

R2 R4 R5

```
!
router ospf 1
 redistribute connected subnets route-map to-ospf
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
route-map to-ospf permit 10
 match interface Loopback1
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
```


R5

R5


R2
R4
R5
cisco
R5>
R5>
R5>en
R5#
R5#
R5#sh run
Building configuration...
Current configuration : 1496 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
--More--
freecram.net
Activate W
Go to Settings

R2 R4 R5

```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
key chain CCNP
 key 1
  key-string CCNP
  cryptographic-algorithm md5
!
!
!
!
```

R2 R4 R5

```
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.5.5 255.255.255.255
 ip ospf 1 area 1
!
interface Loopback1
 ip address 172.16.5.5 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.45.5 255.255.255.0
 ip ospf authentication key-chain CCNP
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/1
 ip address 172.16.45.5 255.255.255.0
 ip ospf 1 area 1
 ip ospf cost 60
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
```

Answer:

See the solution in Explanation below.

Explanation:

SOLUTION:-

R4

Int range et0/0 - 1

Ip ospf authentication message-digest

Ip ospf message-digest-key 1 md5 CCNP

Router ospf 1

Redistribute connected subnets route-map to-ospf metric-type 1

Copy run start

R5

Int range et0/0 - 1

Ip ospf authentication message-digest

Ip ospf message-digest-key 1 md5 CCNP

Interface eth 0/1

Ip ospf cost 10

Copy run start

VERIFICATION:-

A black screen with white text AI-generated content may be incorrect.

NEW QUESTION: 123

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 FastEthemet0/1 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 reported distance greater than the successor's feasible distance.

D. Configure feasible distance greater than the reported distance

Answer: (SHOW ANSWER)

From the exhibit, we notice network 172.29.0.0/16 was learned via two routes:

+ From 192.168.254.2 with FD = 307200 and AD = 281600

+ From 192.168.253.2 with FD = 410200 and AD = 352300

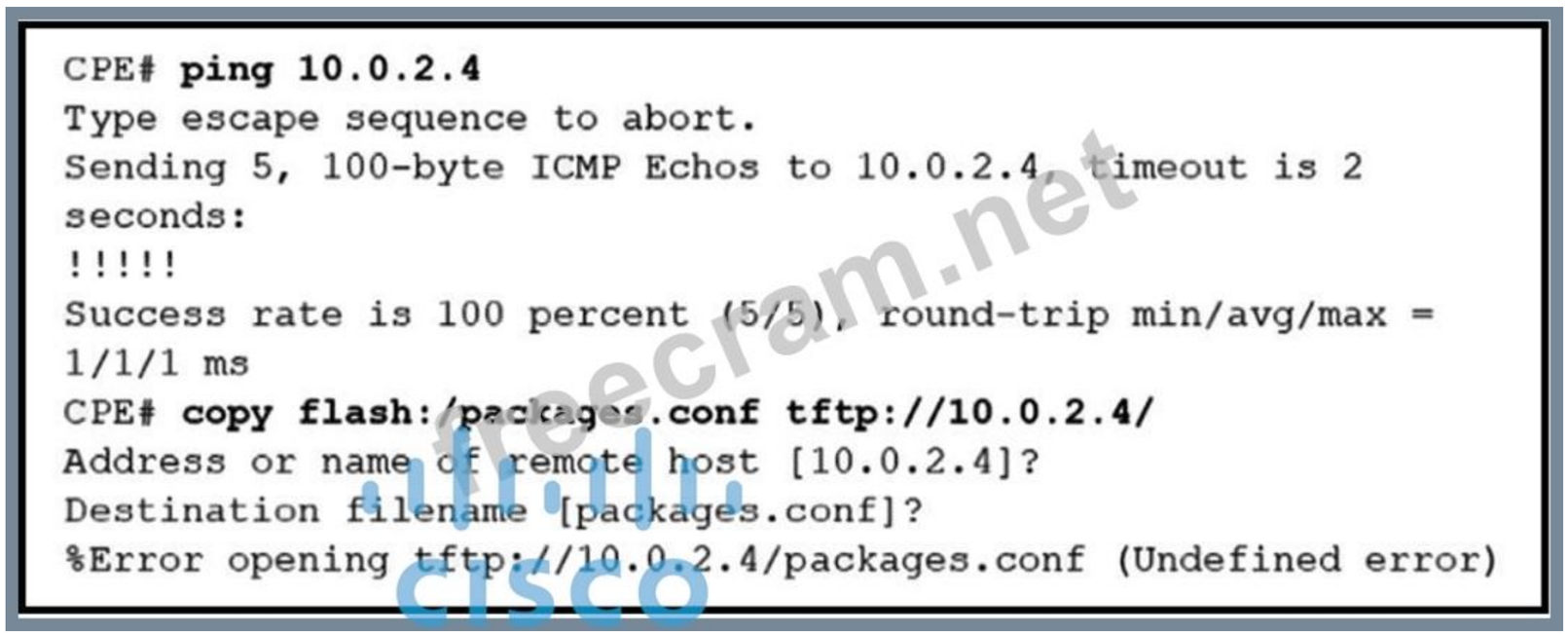
The first route is installed into the RIB as the successor route because of lower FD.

When the first route fails, router will not use the second route as it does not satisfy the feasibility condition.

The feasibility condition states that, the Advertised Distance (AD, also called the reported distance) of a route must be lower than the feasible distance of the current successor route.

NEW QUESTION: 124

Refer to the exhibit.



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 TFTP folder writable by all on the TFTP server

B. Make the packages.conf file executable by all on the TFTP server

C. Make sure to run the TFTP service on the TFTP server

D. Make the packages.conf file writable by all on the TFTP server

Answer: (SHOW ANSWER)

NEW QUESTION: 125

Refer to the exhibit.

```
ipv6 inspect udp idle-time 3600
ipv6 inspect name ipv6-firewall tcp
ipv6 inspect name ipv6-firewall udp
!
ipv6 access-list ipv6-internet
deny ipv6 any FEC0::/10
deny ipv6 any FF00::/8
permit ipv6 any FF02::/16
permit ipv6 any FF0E::/16
permit udp any any eq domain log
!
Interface gi0/1
ipv6 traffic-filter ipv6-internet in
ipv6 inspect ipv6-firewall in
ipv6 inspect ipv6-firewall out
```


A network administrator configured name resolution for IPv6 traffic to be allowed through an inbound access list. After the access list is applied to resolve the issue, name resolution still did not work. Which action does the network administrator take to resolve the name resolution problem?

A. Add permit udp any eq domain any log in the access list.
B. Remove ipv6 inspect ipv6-firewall in from interface gi0/1
C. Add permit any eq domain 53 any log in the access list.
D. inspect ipv6 inspect name ipv6-firewall udp 53 in global config.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126

Refer to the exhibit. Not all connected and static routes of router B are received by router A even though EIGRP neighborship is established between the routers. Which configuration resolves the issue?

A.
```
router eigrp 100
 network 209.165.200.224 0.0.0.7
```

B.
```
router eigrp 100
 network 209.165.200.224 0.0.0.7
 redistribute static metric 1000 1 255 1 1500
 eigrp stub connected
```

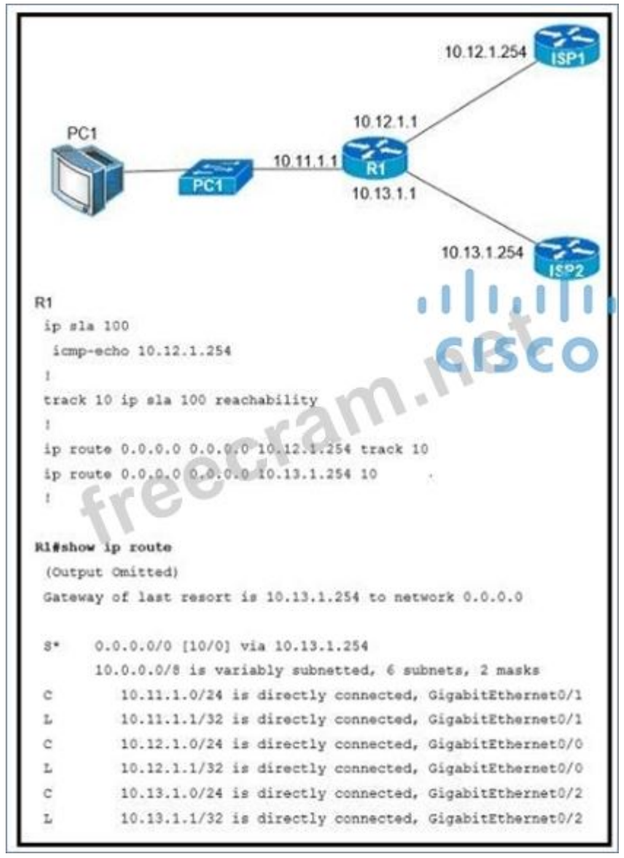
C.
```
router eigrp 100
 network 209.165.200.224 0.0.0.7
 redistribute static metric 1000 1 255 1 1500
 eigrp stub static
```

D.
```
router eigrp 100
 network 209.165.200.224 0.0.0.31
 redistribute static metric 1000 1 255 1 1500
```

Answer: (SHOW ANSWER)

NEW QUESTION: 127

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?

A. Use the icmp-echo command to track both default routes

B. Use the same AD for both default routes

C. Start IP SLA by matching numbers for track and ip sla commands

D. Start IP SLA by defining frequency and scheduling it

Answer: (SHOW ANSWER)

Reference: https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default- routes-using-I.html In the above configuration we have not had activated our IP SLA operation. We can start it with this command:

R1(config)#ip sla schedule 100 life forever start-time now

Also we should specific the rate of ICMP echo:

R1(config-ip-sla-echo)#frequency 5 // Send ICMP echo every 5 seconds

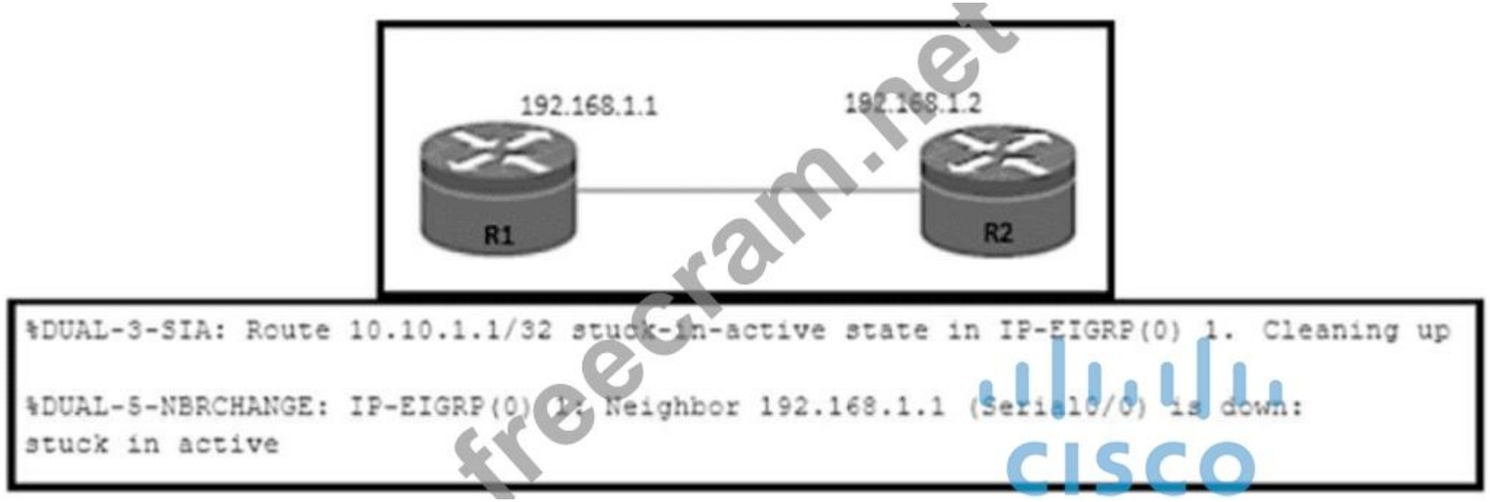
NEW QUESTION: 128

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 input direction

B. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the input direction
C. 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
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 m the output direction
Answer: (SHOW ANSWER)

NEW QUESTION: 129



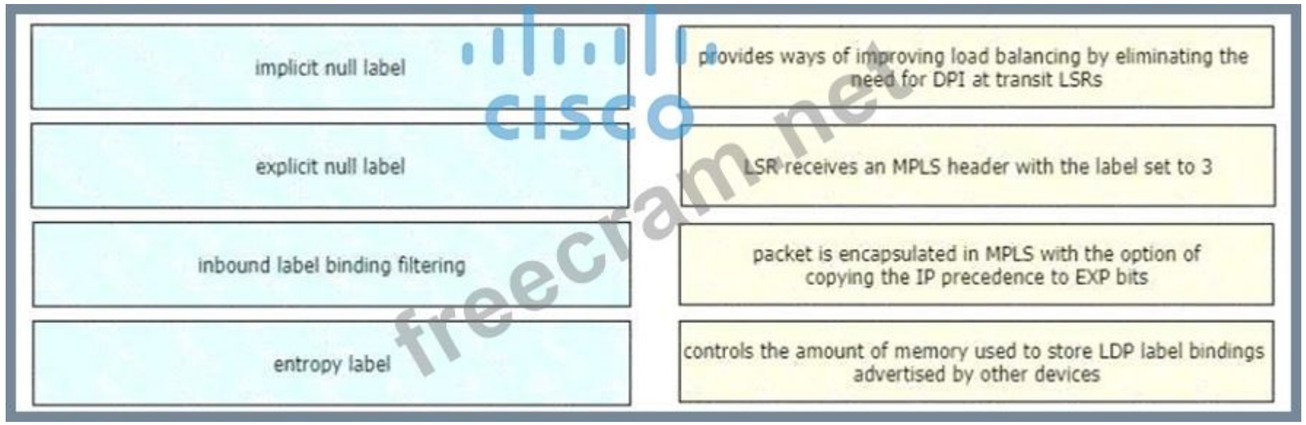
Refer to the exhibit. An engineer notices a connectivity problem between routers R1 and R2. The frequency of this problem is high during peak business hours. Which action resolves the issue?
A. Set static EIGRP neighborship between R1 and R2.
B. Increase the MTU on the interfaces that connect R1 and R2.
C. Decrease the EIGRP keepallve and hold down timers on R1 and R2.
D. Increase the available bandwidth between R1 and R2.
Answer: (SHOW ANSWER)

NEW QUESTION: 130

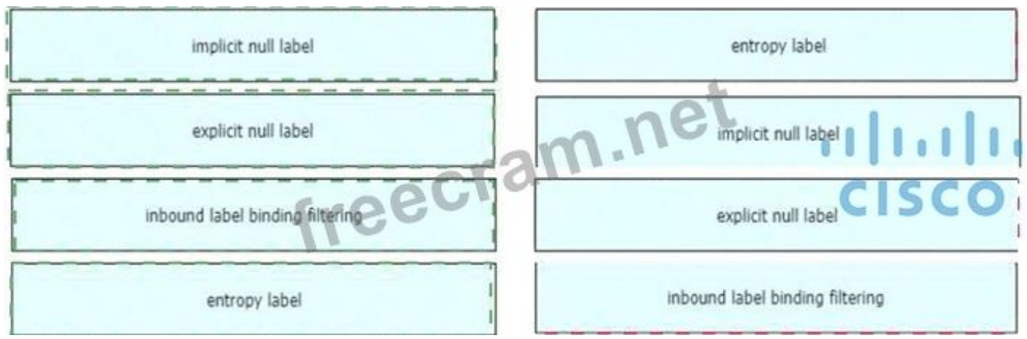
What must be configured by the network engineer to circumvent AS_PATH prevention mechanism in IP /VPN Hub and Spoke deployment scenarios?
A. Use Allowas-in the PE_Hub
B. Use as-override at the PE_Hub
C. Use allows in and as-override at all Pes.
D. Use allowas in and as-override at the PE-Hub.
Answer: (SHOW ANSWER)

NEW QUESTION: 131

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

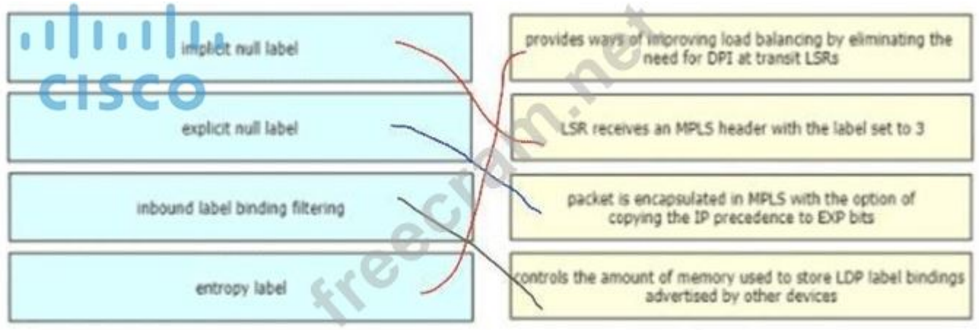


Answer:



Explanation:

Diagram Description automatically generated



The MPLS LDP Inbound Label Binding Filtering feature can be used to control the amount of memory used to store Label Distribution Protocol (LDP) label bindings advertised by other devices. For example, in a simple Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment, the VPN provider edge (PE) devices might require label switched paths (LSPs) only to their peer PE devices (that is, they do not need LSPs to core devices). Inbound label binding filtering enables a PE device to accept labels only from other PE devices.

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-boo k/mp-ldp-inbound-filtr.html

NEW QUESTION: 132

Which method provides failure detection in BFD?
A. short duration, low overhead
B. short duration, high overhead
C. long duration, low overhead
D. long duration, high overhead
Answer: (SHOW ANSWER)

NEW QUESTION: 133
The network administrator configured CoPP so that all SNMP traffic from Cisco Prime located at
192.168.1.11 toward the router CPU is limited to 1000 kbps. Any traffic that exceeds this limit must be dropped.
access-list 100 permit udp any any eq 161
!
class-map CM-SNMP
match access-group 100
!
policy-map PM-COPP
class CM-SNMP
police 1000 conform-action transmit
!
control-plane
service-policy input PM-COPP
The network administrator is not getting the desired result for the SNMP traffic and SNMP traffic is getting dropped frequently. Which set of configurations resolves the issue?
A. no access-list 100access-list 100 permit tcp host 192.168.1.11 any eq 161
B. no access-list 100access-list 100 permit udp host 192.168.1.11 any eq 161!policy-map PM-COPPclass CM-SNMPno police 1000 conform-action transmitpolice 1000000 conform-action transmit!control- planeno service-policy input PM-COPP!interface E 0/0service-policy input PM-COPP!interface E 0
/1service-policy input PM-COPP
C. no access-list 100access-list 100 permit udp host 192.168.1.11 any eq 161!policy-map PM-COPPclass CM-SNMPno police 1000 conform-action transmitpolice 1000000 conform-action transmit
D. policy-map PM-COPPclass CM-SNMPno police 1000 conform-action transmitpolice 1000000 conform- action transmit
Answer: (SHOW ANSWER)
In the context of Control Plane Policing (CoPP) in Cisco devices, the rate limit is specified in bits per second (bps), not kilobits per second (kbps). Therefore, a limit of 1000 kbps should indeed be entered as 1,000,000 bps in the CoPP configuration.
Also, the access list should be configured to match the specific SNMP traffic from the Cisco Prime IP address (192.168.1.11), as you correctly pointed out.
Here's the corrected configuration:
no access-list 100
access-list 100 permit udp host 192.168.1.11 any eq 161
!
policy-map PM-COPP
class CM-SNMP
no police 1000 conform-action transmit
police 1000000 conform-action transmit
This configuration ensures that only the SNMP traffic from Cisco Prime is policed and any excess traffic is dropped, preventing the router's CPU from being overwhelmed.

NEW QUESTION: 134
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, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
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. 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.
B. 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
C. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0.255.0.0.0 command under the Fast Ethernet 0/0 interface.
D. The summarization condition is not met. The network 10.1.100.0/24 should be changed to 172.16.0.0
/24.
Answer: A (LEAVE A REPLY)

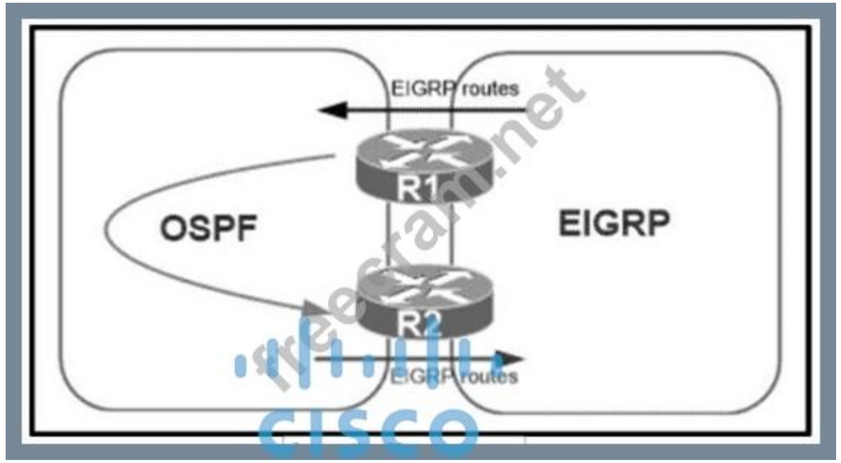
NEW QUESTION: 135
What is the minimum time gap required by the local system before putting a BFD control packet on the wire?
A. Detect Mult
B. Required Min Echo RX Interval
C. Desired Min TX Interval
D. Required Min RX Interval
Answer: (SHOW ANSWER)
Desired Min TX Interval: This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD Control packets, less any jitterapplied. The value zero is reserved.
Required Min Echo RX Interval: This is the minimum interval, in microseconds, between received BFD Echo packets that this system is capable of supporting, less anyjitter applied by the sender. If this value is zero, the transmitting system does not support the receipt of BFD Echo packets.
Reference: https://tools.ietf.org/html/rfc5880

NEW QUESTION: 136
An engineer configured routing between multiple OSPF domains and introduced a routing loop that caused network instability. Which action resolves the problem?
A. Set a tag using the network command in a domain and use the route-map command to deny the matching lag when exiting toward a different domain
B. Set a tag using the redistribute command toward a domain and deny inbound m the other domain by a matching tag
C. Set a tag using the redistribute command toward a different domain and deny the matching tag when exiting from that domain
D. Set a tag using the network command in a domain and use the route-map command to deny the matching tag when entering into a different domain

NEW QUESTION: 137
Which two statements about VRF-Lite configurations are true? (Choose two.)
A. Each customer has its own private routing table.
B. They support a maximum of 512.000 routes
C. Each customer has its own dedicated TCAM resources
D. Different customers can have overlapping IP addresses on different VPNs
E. They support IS-IS
F. They support the exchange of MPLS labels
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which protocol does VRF-Lite support?
A. IS-IS
B. EIGRP
C. ODR
D. IGRP
Answer: (SHOW ANSWER)

NEW QUESTION: 139
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 (LEAVE A REPLY)
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.
html

NEW QUESTION: 140

```
RouterA#show snmp community
 Community name: ILMI
 Community Index: ILMI
 Community SecurityName: ILMI
 storage-type: read-only active

 Community name: ccnp
 Community Index: ccnp Community SecurityName: ccnp
 storage-type: nonvolatile active access-list: 4

RouterA#show ip access-lists
 Standard IP access list 4
 10 permit 172.16.1.1
 20 permit 172.16.2.2
 30 permit 172.16.3.3
Extended IP access list BRANCHES
 10 permit ip 172.16.4.4 any (95 matches)
 20 deny ip any any (95 matches)
```

Refer to the exhibit The SNMP server with IP address 172.16 4 4 cannot access host router A Which configuration command on router A resolves the issue?

A. snmp-server host 172.16.4.4 ccnp
B. access-list 4 permit host 172.16.4.4
C. snmp-server community ccnp
D. access-list 4 permit 172.16.4.0 0.0.0.3

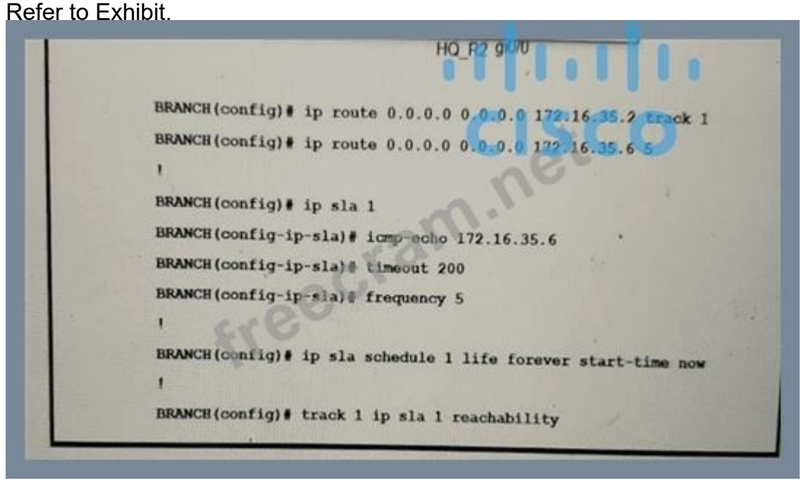
Answer: (SHOW ANSWER)

NEW QUESTION: 141

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 ASBR.
B. Configure the summary-address command on the ABR.
C. Configure the area range command on the ABR.
D. Configure the area range command on the ASBR.
Answer: (SHOW ANSWER)
For OSPF, we can only summary at the ABR with the command "area range" or at the ASBR with the command "summary-address" -> Therefore answer A and answer B are not correct.
In this question, the most likely problem is that when doing summarization, the network mask is configured wrong and summarization doesn't work because of the misconfiguration. When configuring the area range command, make sure that the summarization mask is in the form of a prefix mask rather than a wildcard mask (that is, 255.255.255.0 instead of 0.0.0.255).
Good reference: https://www.configrouter.com/troubleshooting-route-summarization-ospf-14082/

NEW QUESTION: 142
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 3x3 ms hello timer
C. Continuity for each member link of a link aggregation group must be verified
D. Eny member link on a link aggregation group must run BFD
E. Each member link of a link aggregation group must run BFD.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-16-8/irb-xe-16-8-book/irb-micro-bfd.html

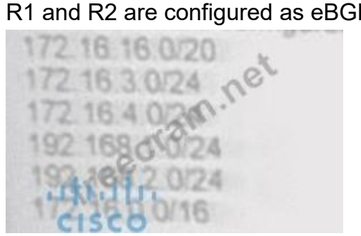
NEW QUESTION: 143
Refer to Exhibit.



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_R1(config)# ip sla responderHQ_R1(config)# ip sla responder icmp-echo 172.16.35.2
B. BRANCH(config)# ip sla 1BRANCH(config-ip-sla)# icmp-echo 172.16.35.1
C. HQ_R2(config)# ip sla responderHQ_R2(config)# ip sla responder icmp-echo 172.16.35.5

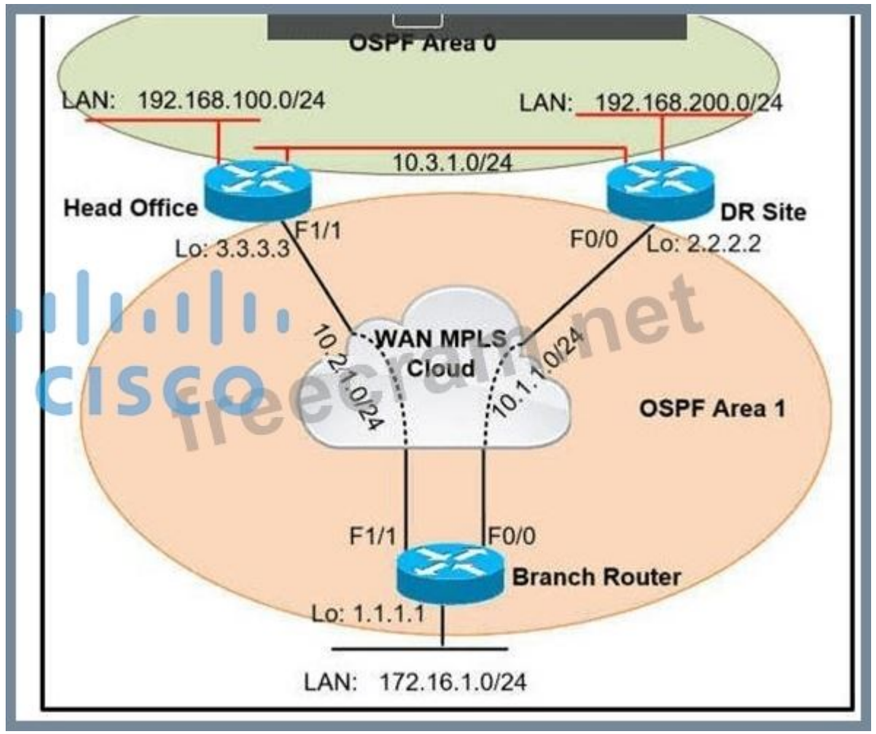
D. BRANCH(config)# ip sla 1BRANCH(config-ip-sla)# icmp-echo 172.16.35.2
Answer: (SHOW ANSWER)
In the configuration above, the engineer has made a mistake as he was tracking 172.16.35.6 (the backup path) instead of tracking the main path (172.16.35.2). Therefore,when he shut down the main path, the track 1 was still up so traffic still went through the main path -> it failed.
To fix this issue, we just need to correct the tracking interface of the main path.

NEW QUESTION: 144
R1 and R2 are configured as eBGP neighbor , R1 is in AS100 and R2 is in AS200. R2 is advertising these networks to R1:



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 23ip prefix-list PL-1 permit 0.0.0.0/0 le 32!router bgp 100neighbor 192.168.100.2 remote-as 200neighbor 192.168.100.2 prefix-list PL-1 in
B. ip prefix-list PL-1 deny 172.16.0.0/16 ge 23ip prefix-list PL-1 permit 0.0.0.0/0 le 32!router bgp 100neighbor 192.168.100.2 remote-as 200neighbor 192.168.100.2 prefix-list PL-1 in
C. access-list 1 deny 172.16.0.0 0.0.254.255access-list 1 permit any!router bgp 100neighbor 192.168.100.2 remote-as 200neighbor 192.168.100.2 distribute-list 1 in
D. ip prefix-list PL-1 deny 172.16.0.0/16ip prefix-list PL-1 permit 0.0.0.0/0!router bgp 100neighbor 192.168.100.2 remote-as 200neighbor 192.168.100.2 prefix-list PL-1 in
Answer: (SHOW ANSWER)
"Blocking all subnets of 172.16.0.0/16 major network with a mask lower than 23 from coming in" would block 172.16.16.0/20.
The first prefix-list "ip prefix-list PL-1 deny 172.16.0.0/16 le 23" means "all networks that fall within the 172.16.0.0/16 range AND that have a subnet mask of /23 or less" are denied.
The second prefix-list "ip prefix-list PL-1 permit 0.0.0.0/0 le 32" means allows all other prefixes.

NEW QUESTION: 145
Refer to the exhibit.



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. Configure matching hello and dead intervals between sites.

B. Advertise the branch WAN interface matching subnet for the DR site.

C. Stabilize the DR site flapping link to establish OSPF adjacency.

D. Configure the WAN interface for DR site in the related OSPF area.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 146

What is an MPLS LDP targeted session?

A. LDP session established between LSRs by exchanging TCP hello packets

B. LDP session established by exchanging multicast 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: (SHOW ANSWER)

NEW QUESTION: 147

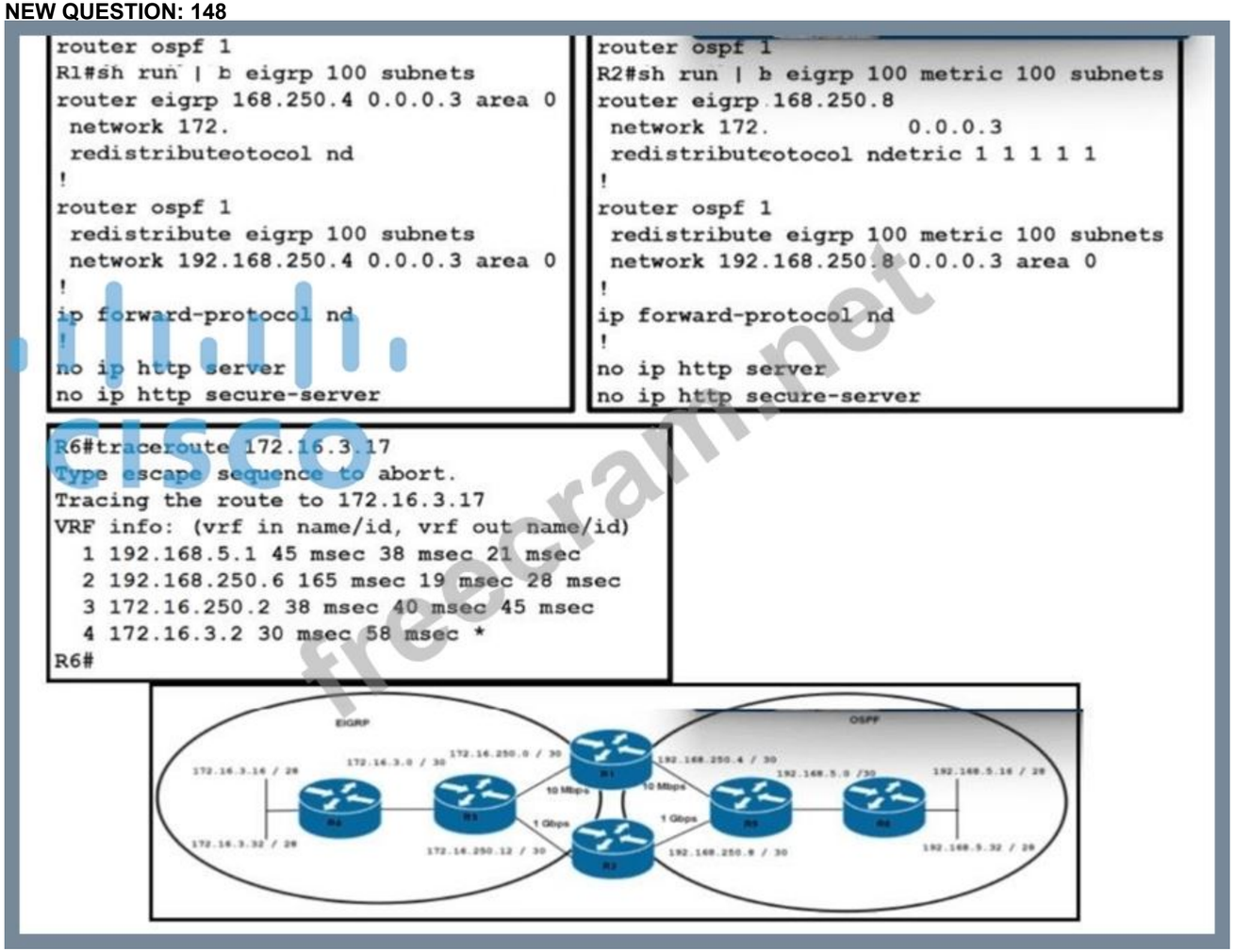
An engineer configured SNMP notifications sent to the management server using authentication and encrypting data with DES. An error in the response PDU is received as "UNKNOWNUSERNAME. WRONGDIGEST". Which action resolves the issue?

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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

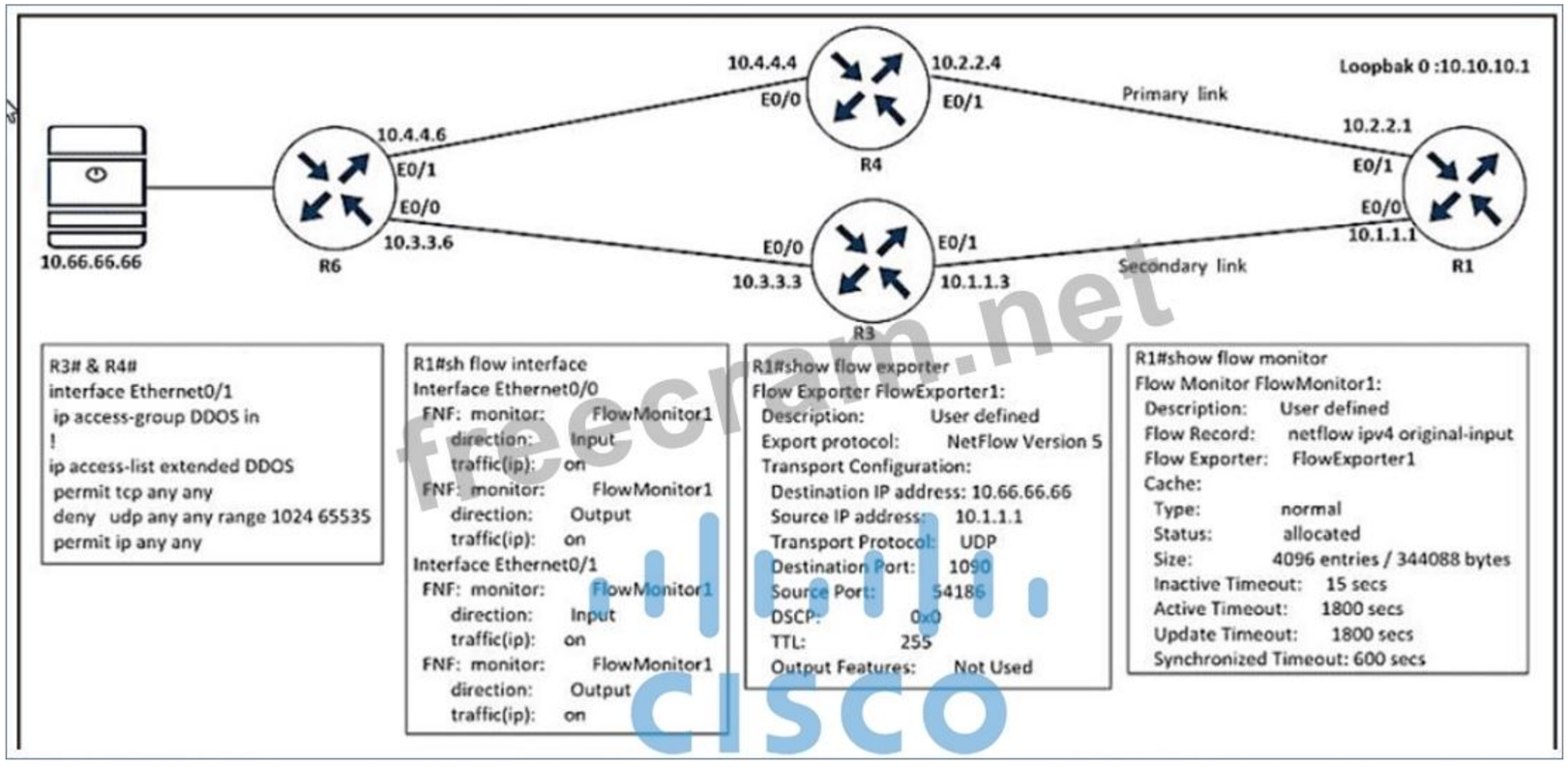
NEW QUESTION: 148



Refer to the exhibit. An engineer is troubleshooting suboptimal communication from the 192.168.5.32/28 subnet to the 172.16.3.16/28 segment using the slowest links. Which configuration resolves the suboptimal routing issue?
A. R2(config-router)#ro uter ospf 1
R2(config-router)#default-metric 10
R1(config-router)#router ospf 1
R1(config-router)#default-metric 1
B. R2{config-router)#router ospf 1

R2{config-roiiter)#default-metric 1
R1(config-router)#router ospf 1
R1(config-router)#default-metric 10
C. R1(config-router)#router elgrp 100
R1(config-router)#redistribute ospf 1 metric 1000000 1111
D. R2(config-router)#ro liter eigrp 100
R2(config-router)#redistribute ospf 1 metric 1000000 1111
Answer: (SHOW ANSWER)

NEW QUESTION: 149



Refer to the exhibit An engineer configured NetFlow but cannot receive the flows from R1 Which two configurations resolve the issue? (Choose two)

A.
```
R1(config)#flow exporter FlowExporter1
R1(config-flow-exporter)#destination 10.66.60.66
```

B.
```
R3(config)#flow exporter FlowExporter1
R3(config-flow-exporter)#destination 10.66.66.66
```

C.
```
R4(config)#ip access-list extended DDOS
R4(config-ext-nacl)#5 permit udp any host 10.66.66.66 eq 1090
```

D.
```
R3(config)#ip access-list extended DDOS
R3(config-ext-nacl)#5 permit udp any host 10.66.66.66 eq 1090
```

E.
```
R4(config)#flow exporter FlowExporter1
R4(config-flow-exporter)#destination 10.66.66.66
```

Answer: (SHOW ANSWER)

NEW QUESTION: 150

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: (SHOW ANSWER)

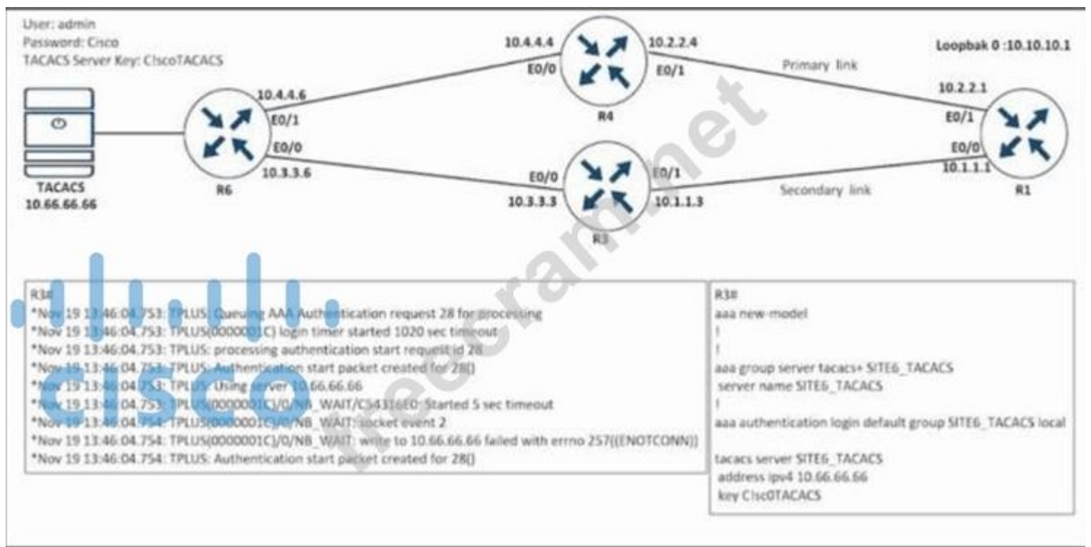
According to this question, uRPF is running in strict mode because packets are dropped even when that route exists in the routing table. Maybe packets are dropped because the receiving interface is different from the interface the local router uses to send packets to that destination.

The ip verify unicast source reachable-via rx command enables Unicast RPF in strict mode.

To enable loose mode, administrators can use the any option (ip verify unicast source reachable-via any). In loose mode, it doesn't matter if we use this interface to reach the source or not.

The allow-default option allows the use of the default route in the source verification process.

NEW QUESTION: 151



Refer to the exhibit. R3 cannot authenticate via TACACS. Which configuration resolves the issue?

A. tacacs server SITE6_TACACS
key C!scOTACACS
address ipv4 10.60.66.66

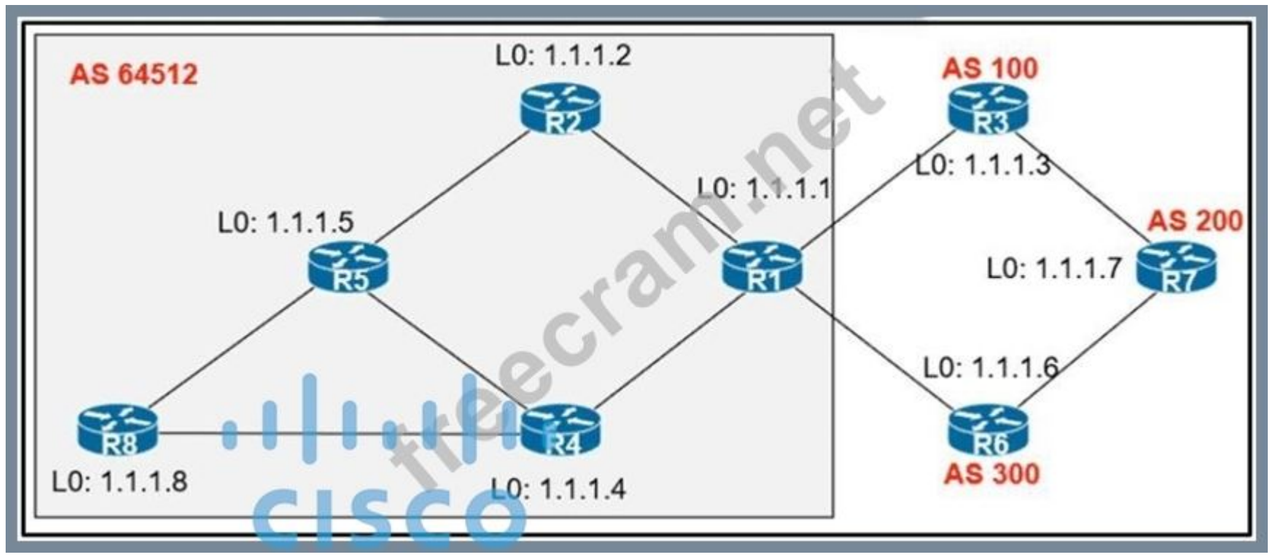
B. tacacs server SITE6_TACACS
key CiscoTACACS
address ipv4 10.66.66.66

C. tacacs server SITE6_TACACS
key CIscoTACACS

D. tacacs server SITE6_TACACS
key C!scoTACACS
address ipv4 10.60.66.66

Answer: (SHOW ANSWER)

NEW QUESTION: 152
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: (SHOW ANSWER)

When R2 & R5 are route reflectors (RRs), routes from R4 & R8 are advertised to R5 and R5 advertises to R2. But R2 would drop them as R2 is also a RR. Therefore some routes are missing on R1 to advertise to eBGP peers.

Good reference:

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/TECRST-2310.pdf Route reflectors (RR) must be fully iBGP meshed so we cannot configure RR on both R1 and R5.

We should choose routers at the center of the topology RRs, in this case R4 & R5.

NEW QUESTION: 153

Which protocol is used to determine the NBMA address on the other end of a tunnel when mGRE is used?

A. OSPF

B. IPsec

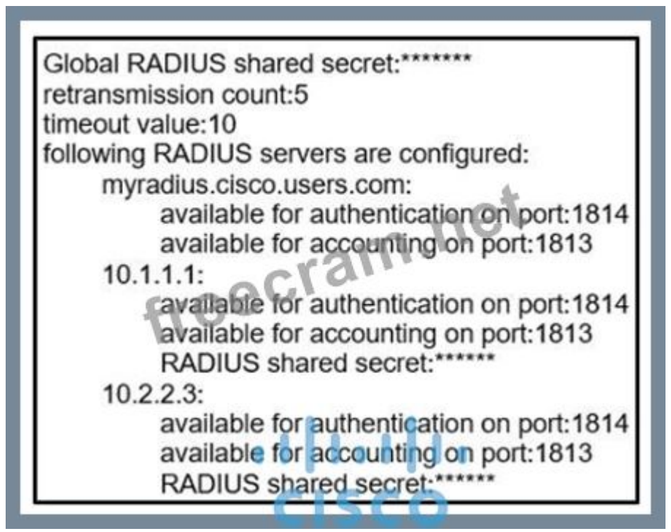
C. MP-BGP

D. NHRP

Answer: (SHOW ANSWER)

NEW QUESTION: 154

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?

A. Match the authentication port

B. Match the accounting port

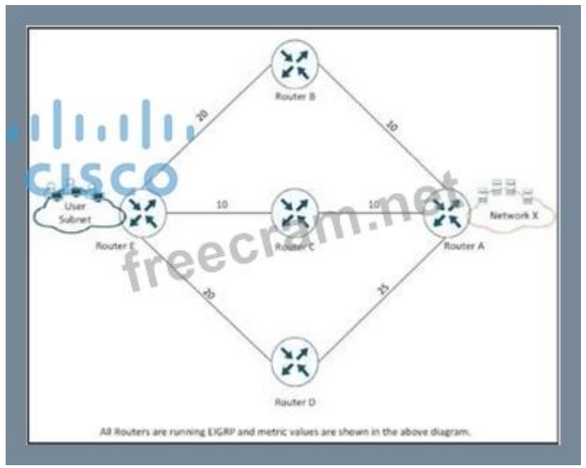
C. Correct the timeout value.

D. Correct the shared secret.

Answer: (SHOW ANSWER)

Command Default
Accounting port: 1813
Authentication port: 1812
Accounting: enabled
Authentication: enabled
Retransmission count: 1
Idle-time: 0
Server monitoring: disabled
Timeout: 5 seconds
Test username: test
Test password: test
Reference:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/radius-server-host.html By default, RADIUS uses UDP port 1812 for authentication and port 1813 for accounting. In the exhibit above we see port 1814 is being used for authentication to AAA server at 10.1.1.1 which is not the default port so we must adjust the authentication port to the default value 1812.

NEW QUESTION: 155



Refer to the exhibit. The IT manager received reports from users about slow application through network x.
which action resolves the issue?

A. Use the variance 2 command to enable load balancing.

B. Upgrade the IOS on router E.

C. Increase the bandwidth from the service provider.

D. Move the servers into the users subnet.

Answer: (SHOW ANSWER)

NEW QUESTION: 156

Exhibit:

```
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
```

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

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: (SHOW ANSWER)

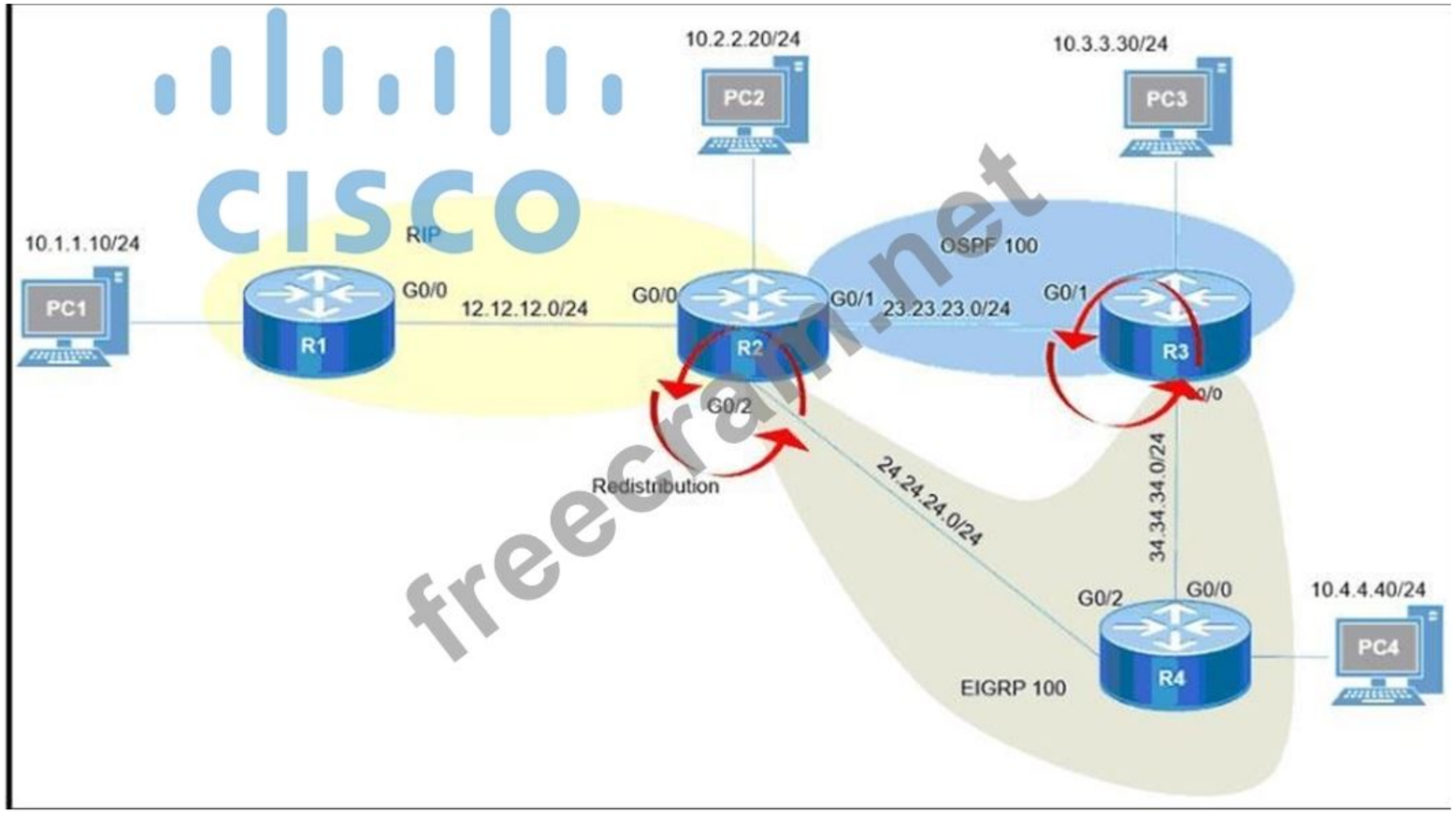
The policy-map COPP-7600 only rate-limit HTTP & HTTPS traffic (based on the ACL conditions) so any BGP packets will be processed in the class "class-default", which drops exceeded BGP packets. Therefore we have two ways to solve this problem:

+ Add BGP to the ACL with the statement "permit tcp any any eq bgp"

+ Configure higher value for CIR in default class as 2Mbps is too low for web traffic (http & https)

NEW QUESTION: 157

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. Redistribute the directly connected interfaces on R2.

B. Set the administrative distance 100 under the RIP process on R2.

C. Filter the prefix 10.1.1.0/24 when redistributed from OSPF to EIGRP.

D. Filter the prefix 10.1.1.0/24 when redistributed from RIP to EIGRP.

Answer: (SHOW ANSWER)

NEW QUESTION: 158

:589

Aswitchhas been configured to provide DHCP relay on VLAN 100 to a server with an IP address of 10.1.1.1.

The DHCP server is sending syslog reports of multiple TFTP requests that also originate from the switch. As a result, the server CPU exceeded a configured threshold. Which action does the network administrator recommend to bring the server CPU threshold down?

A. Configure the switch with ip forward-protocol udp 67 globally.

B. Configure the switch with an access list on VLAN100 to deny TFTP.

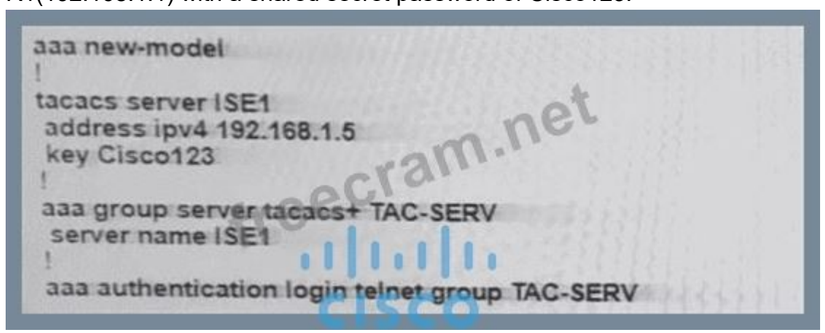
C. Configure the switch with a VACL on VLAN100 to deny TFTP.

D. Configure the switch with no ip forward-protocol udp 69 on VLAN100.

Answer: (SHOW ANSWER)

NEW QUESTION: 159
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 slow or disconnects frequently.
Which command must be configured first to troubleshoot this issue?
A. show policy-map
B. show interface | inc drop
C. show ip route
D. show policy-map control-plane
Answer: (SHOW ANSWER)

NEW QUESTION: 160
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.

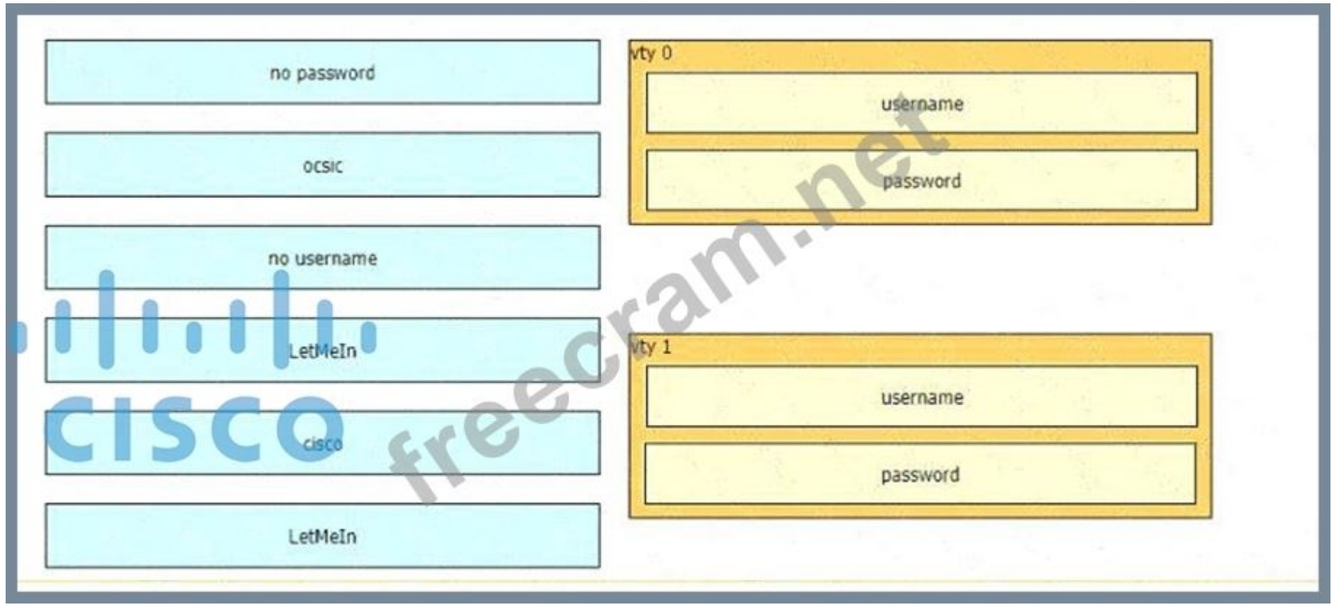


The administrator cannot authenticate to R1 based on ISE. Which configuration fixes the issue?
A. ip tacacs-server host 192.168.1.5 key Cisco123
B. line vty 0 4login authentication TAC-SERV
C. line vty 0 4login authentication telnet
D. tacacs-server host 192.168.1.5 key Cisco123
Answer: (SHOW ANSWER)
The last command "aaa authentication login telnet group TAC-SERV" created the method list name telnet so we need to assign it to line vty.
Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208- Configure-ISE-2-0-IOS-TACACS-Authentic.html

NEW QUESTION: 161
Refer to the exhibit.

```
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
```

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 uf SLA by defining frequency and schedulingsed



Answer:

Explanation:
vty 0:
+ cisco
+ 0csic
vty 1:
+ no username
+ no password
The command "aaa authentication login default none" means no authentication is required when access to the device via Console/VTY/AUX so if one interface does not specify another login authentication method (via the "login authentication ..." command), it will allow to access without requiring username or password. In this case VTY 1 does not specify another authentication login method so it will use the default method (which is "none" in this case).

NEW QUESTION: 162
What is a function of IPv6 Source Guard?
A. It works with address glean or ND to find existing addresses.
B. It inspects ND and DHCP packets to build an address binding table.
C. It denies traffic from known sources and allocated addresses.
D. It notifies the ND protocol to inform hosts if the traffic is denied by it.
Answer: (SHOW ANSWER)
IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets;rather, it works in conjunction with IPv6 neighbor discovery (ND) inspection or IPv6 address glean, both of which detect existing addresses on the link and store them into the binding table.

NEW QUESTION: 163
Refer to the exhibit.

R1 test its directly connected EIGRP peer 172.16.33.2 (SW1). Which configuration resolves the issue1?

A. key chain EIGRP key 1 key-string Cisco !interface Gigabit Ethernet 2.10 IP authentication mode elgrp 88 md5 IP authentication key-chain eigrp 88 EIGRP

B. key chain EIGRP key1 key-string Cisco !interface Gigabit Ethernet 2 IP authentication mode eigrp 88 md5 IP authentication key-chain elgrp 88 Cisco

C. key chain EIGRP key 1 key-string Cisco!interface Gigabit Ethernet 2 IP authentication mode elgrp 88 md5 IP authentication key-chain elgrp 88 EIGRP

D. key chain EIGRP key1 key-string Cisco!interface Gigabit Ethernet 2.10 IP authentication mode eigrp 88 md5 IP authentication key-chain eigrp 88 Cisco

Answer: (SHOW ANSWER)

NEW QUESTION: 164

Refer to the exhibit.

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

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

A client is concerned that passwords are visible when running this show archive log config all.

Which router configuration is needed to resolve this issue?

A. MASS-RTR(config-archive-log-cfg)#password encryption aes

B. MASS-RTR(config)#aaa authentication arap

C. MASS-RTR(config)#service password-encryption

D. MASS-RTR(config-archive-log-cfg)#hidekeys

Answer: (SHOW ANSWER)

Step 7 | hidekeys

Example:

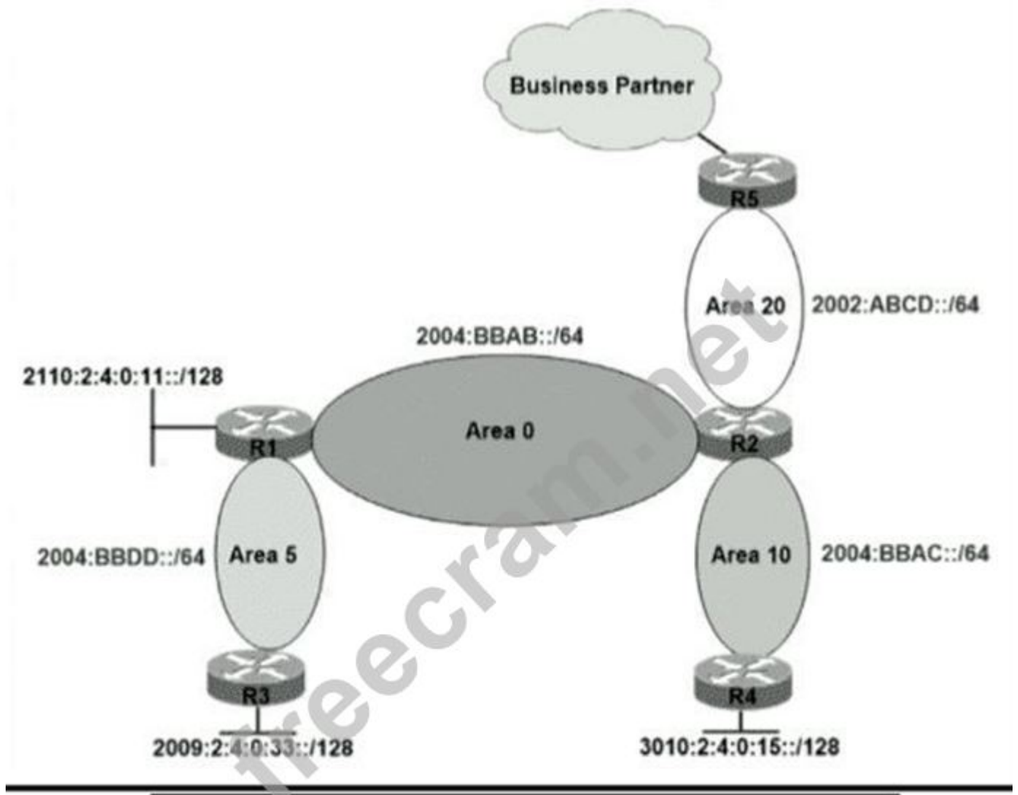
```
Device(config-archive-log-config)# hidekeys
```

(Optional) Suppresses the display of password information in configuration log files.

Note Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.

NEW QUESTION: 165
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: (SHOW ANSWER)
The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link,and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.The feature enables the filtering of IPv6 traffic based on the destinationaddress, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknowndestination.
Reference: https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide
/7600_15_0s_book/IPv6_Security.pdf

NEW QUESTION: 166
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:FE20:8, 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 5 on router R1

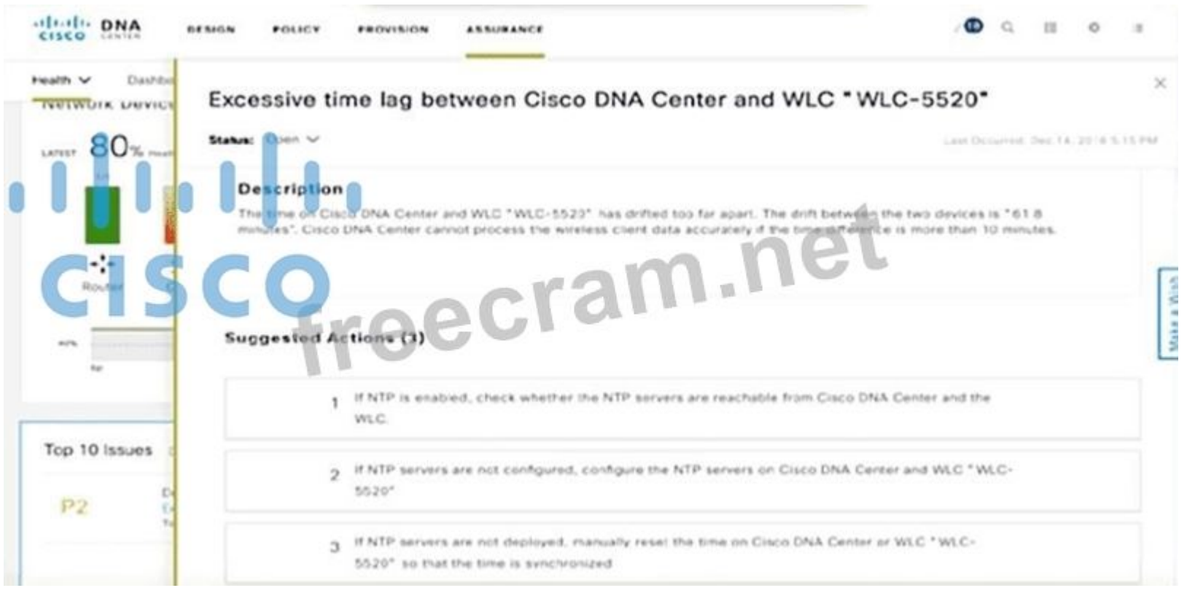
B. in the "out" direction for area 20 on router R2

C. in the "in" direction for area 20 on router R2

D. in the "in" direction for area 5 on router R1

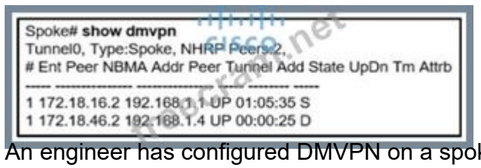
Answer: (SHOW ANSWER)

NEW QUESTION: 167
Exhibit:



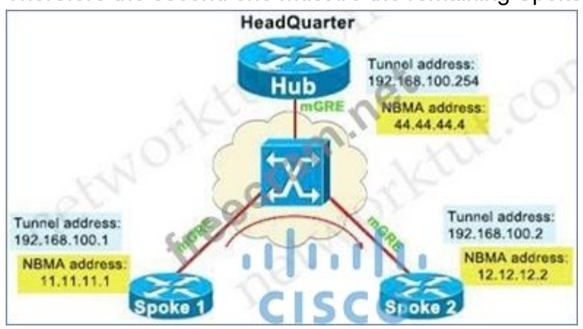
NTP is configured across the network infrastructure and Cisco DNA Center. An NTP issue was reported on the Cisco DNA Center at 17:15. Which action resolves the issue?
A. Check and resolve reachability between the WLC and the NTP server
B. Reset the NTP server to resolve any synchronization issues for 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: (SHOW ANSWER)
Excessive time lag between Cisco DNA Center and device: The time difference between Cisco DNA Center and the device IP Address has drifted too far apart. CiscoDNA Center cannot process the device data accurately if the time difference is more than 3 minutes.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and- management/dna-center-assurance/1-2-10/b_cisco_dna_assurance_1_2_10_ug /b_cisco_dna_assurance_1_2_10_ug_chapter_01101.html

NEW QUESTION: 168
Refer to the exhibit.



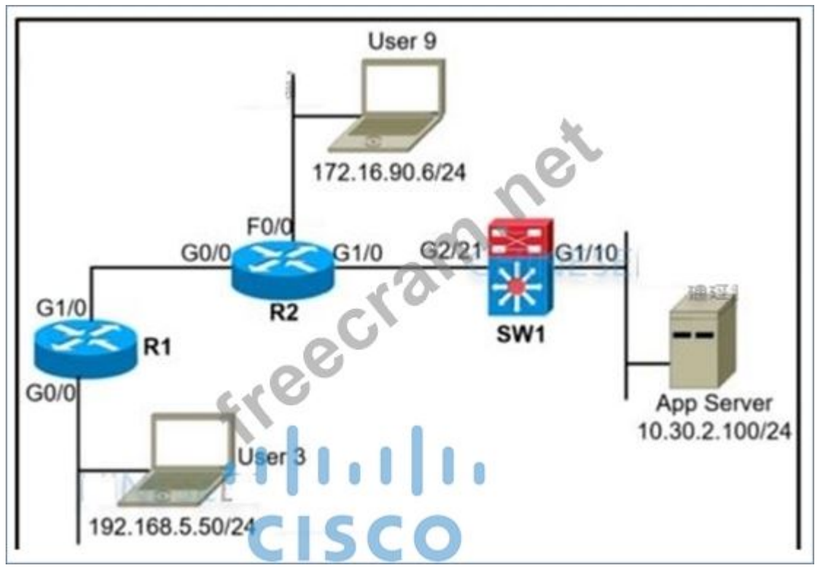
An engineer has configured DMVPN on a spoke router. What is the WAN IP address of another spoke router within the DMVPN network?

A. 172.18.46.2
B. 192.168.1.4
C. 172.18.16.2
D. 192.168.1.1
Answer: (SHOW ANSWER)
From the output we can see there are 2 NHRP Peers. The first one with the NBMA Address of 172.18.16.2 and the "Attribute" (Attrb) of Static (S) so we can deduce it is the Hub device.
Therefore the second one must be the remaining Spoke device with the attribute of Dynamic (D).



--> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==
Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,
Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- ---------- ---------- ----- -------- -----
1 44.44.44.4 192.168.100.254 UP 00:03:40 S
1 12.12.12.2 192.168.100.2 UP 00:03:20 D

NEW QUESTION: 169
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. R2 interface G1/0

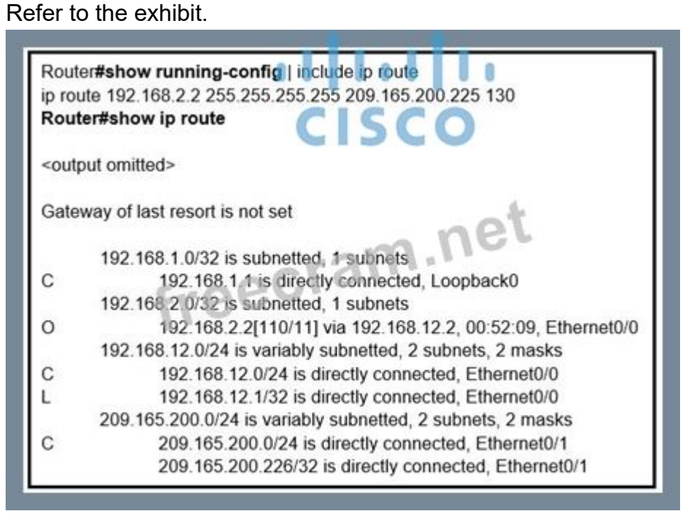
C. SW1 interface G1/10

D. SW1 interface G2/21

Answer: (SHOW ANSWER)

NEW QUESTION: 170

Refer to the exhibit.



An engineer configures 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?

A. Dynamic routing protocols always have priority over static routes.
B. The metric of the OSPF route is lower than the metric of the static route.
C. The configured AD for the static route is higher than the AD of OSPF.
D. The syntax of the static route is not valid, so the route is not considered.
Answer: (SHOW ANSWER)
The AD of static route is manually configured to 130 which is higher than the AD of OSPF router which is 110.

NEW QUESTION: 171
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 (LEAVE A REPLY)
The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform. Router Advertisements are used by devices to announce themselves on the link. The IPv6 Router Advertisement Guard feature analyzes these router advertisements and filters out router advertisements that are sent by unauthorized devices.
Certain switch platforms can already implement some level of rogue RA filtering by the administrator configuring Access Control Lists (ACLs) that block RA ICMP messages that might be inbound on "user" ports.
Reference: https://datatracker.ietf.org/doc/html/rfc6104

NEW QUESTION: 172
Which component of MPLS VPNs is used to extend the IP address so that an engineer is able to identify to which VPN it belongs?
A. VPNv4 address family
B. RD
C. RT
D. LDP
Answer: (SHOW ANSWER)

- Specify the correct route distinguisher used for that VPN. This is used to extend the IP address so that you can identify which VPN it belongs to.

```
rd <VPN route distinguisher>
```

NEW QUESTION: 173
Refer to the exhibit.

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: (SHOW ANSWER)

In the debug output, we see that the Authorization (not Authentication) failed so we need to correct the authorization. In order to enable authorization, we must use the global command "aaa authorization console" first.

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-a1.html

NEW QUESTION: 174

Which configuration adds an IPv4 interface to an OSPFv3 process in OSPFv3 address family configuration?

A. Router ospf3 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: (SHOW ANSWER)

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s- book/ip6-route-ospfv3-add-fam-xe.html

NEW QUESTION: 175

Refer to the exhibit.

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            90.0.1.1        YES NVRAM  up                    up
Ethernet1/0            118.8.10.1      YES NVRAM  up                    up
Loopback6              10.1.7.6        YES NVRAM  up                    up
Loopback7              10.1.7.7        YES NVRAM  up                    up

Router# show ip bgp
BGP table version is 10, local router ID is 10.1.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         0.0.0.0                  0         32768 ?
*> 10.1.7.7/32      0.0.0.0                  0         32768 i
*> 90.0.0.0         0.0.0.0                  0         32768 ?
r> 90.0.1.0/24      100.0.1.254              0             0 6 ?
*> 118.0.0.0        0.0.0.0                  0         32768 ?
r>i118.8.10.0/24    118.8.10.254             0           100 0 ?
```

Which action adds the 10 1 7.6-32 route to the BGP table?

A. Add a static roue for the 10 1 7 &32 network

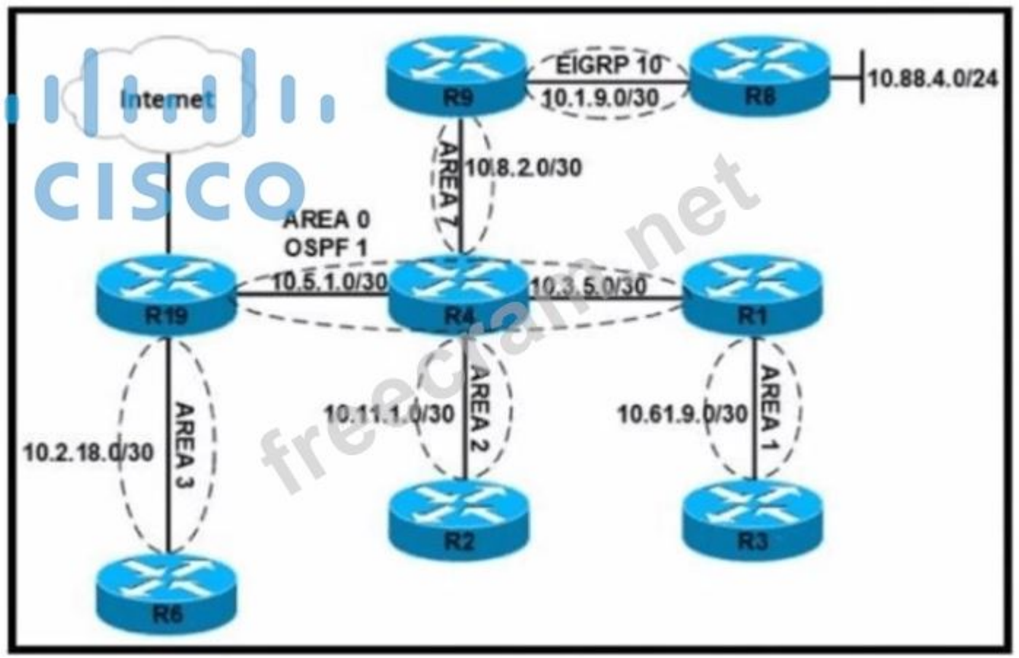
B. Add the network 10.1.7.6 mask 255.255.255.255 command

C. Add the network 10.1.7.6 mask 255.255.255.255 backdoor command

D. Add summaty-address10.1.7.6.255.255.2550

Answer: (SHOW ANSWER)

NEW QUESTION: 176



Refer to the exhibit After an engineer modified the configuration for area 7 to permit type 1 2 and 7 LSAs only users connected to router R9 reported that they could no longer access the internet. Which configuration restores internet access to users on R9 and permits only LSA type 1,2, and 7?

A.
```
R4#
router ospf 1
  area 0 nssa default-information-originate
  network 10.5.1.0 0.0.0.3 area 0
  network 10.8.2.0 0.0.0.3 area 7

R9#
router ospf 1
  area 7 nssa
  redistribute eigrp 10 subnets
  network 10.8.2.0 0.0.0.3 area 7
```

B.
```
R4#
router ospf 1
  area 7 nssa no-summary
  network 10.5.1.0 0.0.0.3 area 0
  network 10.8.2.0 0.0.0.3 area 7

R9#
router ospf 1
  area 7 nssa
  redistribute eigrp 10 subnets
```

C.
```
R4#
router ospf 1
  area 7 nssa
  network 10.5.1.0 0.0.0.3 area 0
  network 10.8.2.0 0.0.0.3 area 7

R9#
router ospf 1
  area 7 nssa
  redistribute eigrp 10 subnets
  network 10.8.2.0 0.0.0.3 area 7
```

D.
```
R4#
router ospf 1
  area 0 area 7 stub no-summary
  network 10.5.1.0 0.0.0.3 area 0
  network 10.8.2.0 0.0.0.3 area 7

R9#
router ospf 1
  area 7 stub
  redistribute eigrp 10 subnets
  network 10.8.2.0 0.0.0.3 area 7
```

Answer: (SHOW ANSWER)

Option B configures area 7 as a not-so-stubby area (NSSA) with the no-summary option on the area border router (ABR) R4. This allows the injection of external routes from EIGRP into the OSPF domain as type 7 LSAs, while preventing the propagation of inter-area summary LSAs into area 7. The no-summary option also generates a default summary route for area 7, which can be used by R9 to reach the internet2.

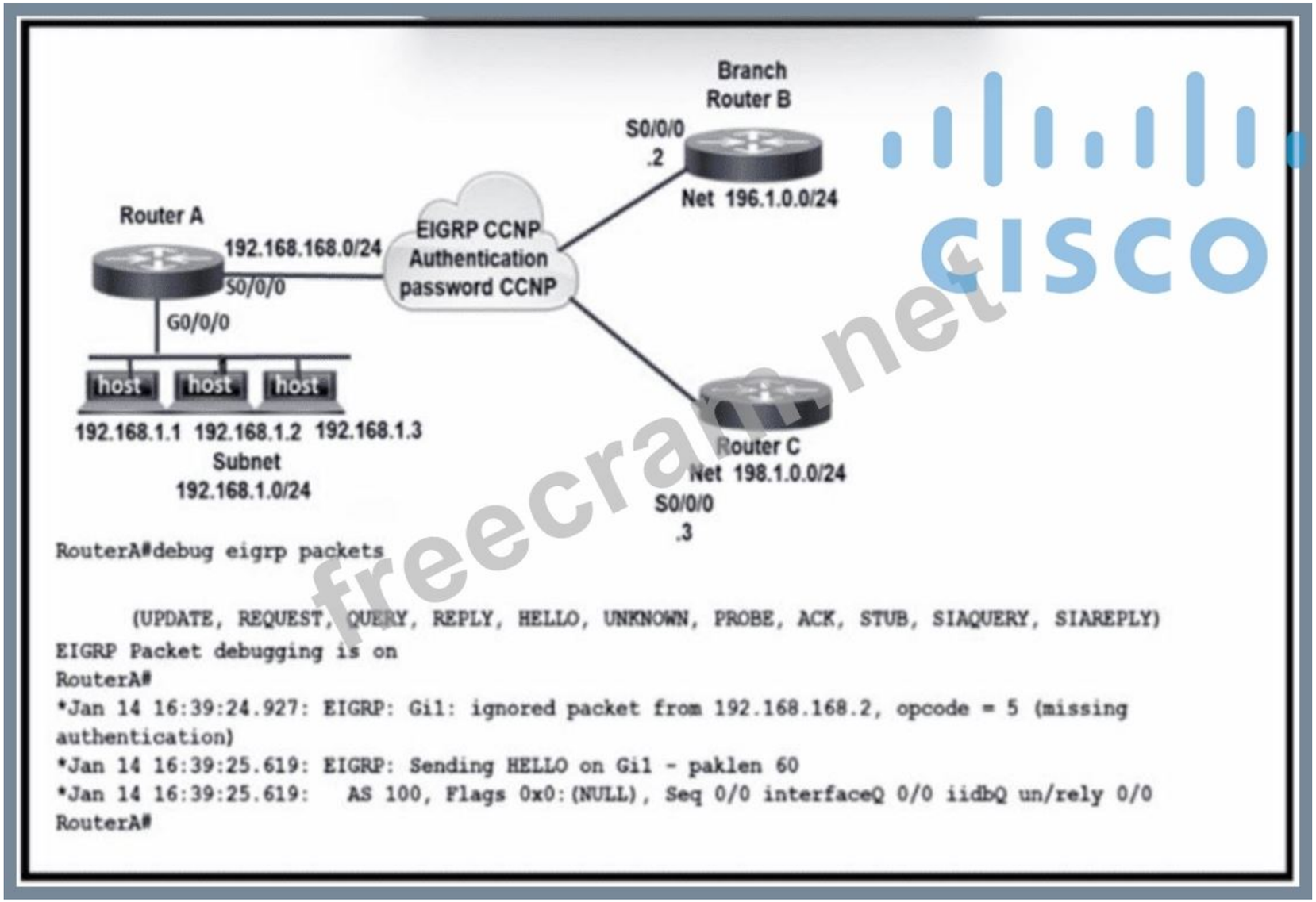
Option A configures area 7 as a stub area, which does not allow any external routes or type 7 LSAs in the area. This prevents R9 from learning the EIGRP routes and accessing the internet3.
Option C configures area 7 as a NSSA without the no-summary option on R4. This allows the injection of type 7 LSAs into the area, but also allows the propagation of inter-area summary LSAs into the area. However, this option does not generate a default summary route for area 7, which means R9 has no route to reach the internet4.
Option D configures area 7 as a NSSA with the default-information originate option on R4. This allows the injection of type 7 LSAs into the area, but also allows the propagation of inter-area summary LSAs into the area. The default-information originate option generates a type 7 default route for area 7, which can be used by R9 to reach the internet. However, this option is redundant and less efficient than Option B, because it injects both a type 3 and a type 7 LSA for the default route into the area5.

NEW QUESTION: 177
Refer to the exhibit.

```
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#
```

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?
A. Add the aaa authentication login default none command to the global configuration.
B. Replace the capital "C" with a lowercase "c" in the aaa authentication login Console local command.
C. Add the aaa authentication login default group tacacs+ local-case command to the global configuration.
D. Add the login authentication Console command to the line configuration
Answer: (SHOW ANSWER)
Reference:
https://community.cisco.com/t5/switching/how-to-define-login-local-for-console-0/td-p/2949493

NEW QUESTION: 178



Refer to the exhibit. The services at branch B are down. An engineer notices mal rouler A and router B are not exchanging any routes Which configuration resolves the issue on router B?

A.

```
router eigrp 100
  network 192.168.168.0

key chain EIGRP
  key 1
    key-string CCNP

interface serial0/0/0
  ip address 192.168.168.2 255.255.255.0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  negotiation auto
```

B.

```
router eigrp 100
  network 192.168.168.0

key chain EIGRP
  key 1
    key-string CCNP

interface serial0/0/0
  ip address 192.168.168.2 255.255.255.0
  ip authentication key-chain eigrp 100 EIGRP
  negotiation auto
```

C.

```
router eigrp 100
  network 192.168.168.0

key chain EIGRP
  key 1
   key-string CCNP

interface serial0/0/0
  ip address 192.168.168.2 255.255.255.0
  ip authentication mode eigrp 100 md5
  negotiation auto
```

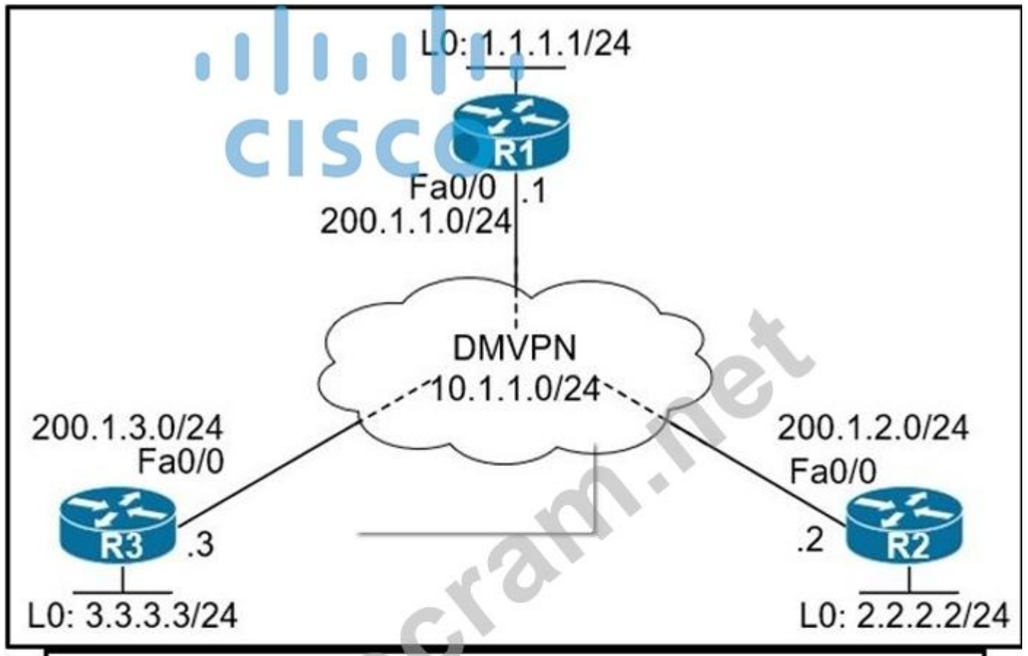
```
router eigrp 100
  network 192.168.168.0

key chain CCNP
  key 1
    key-string EIGRP

interface serial0/0/0
  ip address 192.168.168.2 255.255.255.0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 EIGRP
  negotiation auto
```

D.

Answer: (SHOW ANSWER)

NEW QUESTION: 179

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 a 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.

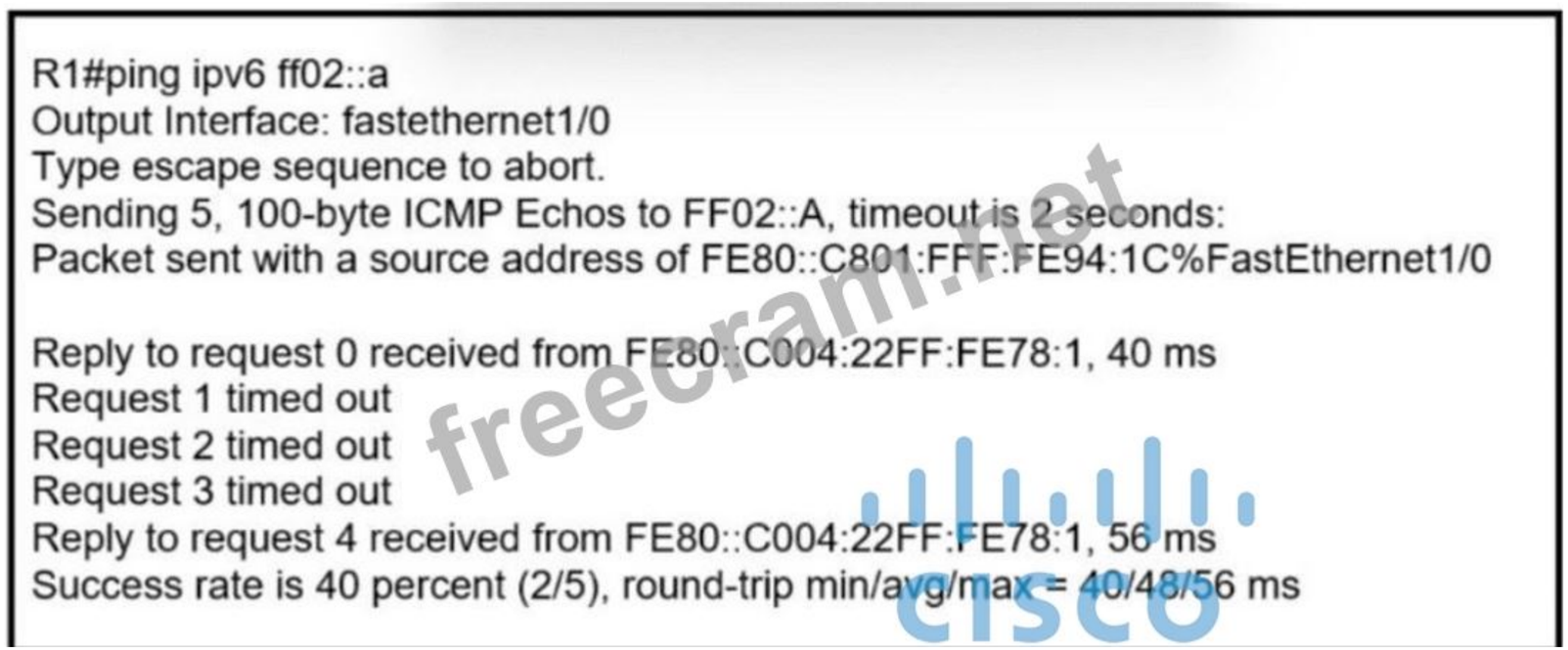
D. Configure crypto isakmp key cisco address 0.0.0.0 on the spokes.

Answer: (SHOW ANSWER)

https://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd802b8f3c.html

NEW QUESTION: 180

:592



Refer to the exhibit An engineer investigates an IPv6 EIGRP neighbor adjacency issue that sees the neighbors flapping and issued a ping from R1 to its directly connected neighbor. The link between the switches is stable at Layer 2. and other connected devices are also functioning. Which action resolves the issue?

A. Data is not reliably transmitted between the dynamically assigned link-local addresses of the routers and must be manually assigned.

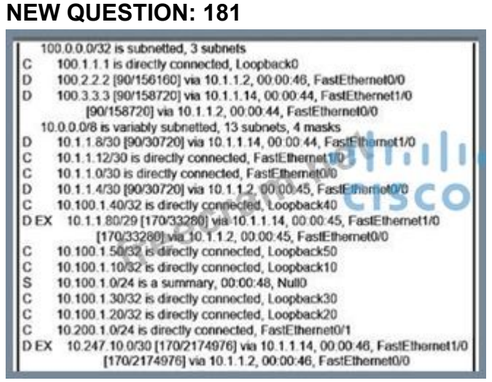
B. Multicast packets are not reliably transmitted over the link, and the switch must be replaced.

C. The switch between the two neighbors is not IPv6 compatible and must be replaced with an IPv6 compatible device.

D. The switch between the two neighbors is not configured for IPv6 multicast and must be configured for IPv6 multicast.

Answer: (SHOW ANSWER)

NEW QUESTION: 181



Refer to the exhibit. R1 must advertise all loopback interfaces IP addresses to neighbors, but EIGRP neighbors receive a summary route. Which action resolves the issue?

A. Redistribute connected routes into EIGRP Enable

B. Disable auto summarization on R1.

C. EIGRP on loopback Interfaces.
D. Remove the 10.100.1.0/24 static route.
Answer: (SHOW ANSWER)

NEW QUESTION: 182
Which two components are required for MPLS Layer 3 VPN configuration? (Choose two)
A. Use OSPF between PE and CE
B. Use LDP for customer routes
C. Use pseudowire for Layer 2 routes
D. Use MP-BGP for customer routes
E. Use a unique RD per customer VRF
Answer: (SHOW ANSWER)

NEW QUESTION: 183
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 access-list 1 permit 10.1.1.0.0.0.0.3.
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 10 and match access-list 1.
E. Configure route-map Leak-Route permit 20.
Answer: (SHOW ANSWER)
When you configure an EIGRP summary route, all networks that fall within the range of your summary are suppressed and no longer advertised on the interface. Only the summary route is advertised. But if we want to advertise a network that has been suppressed along with the summary route then we can use leak-map feature. The below commands will fix the configuration in this question:
R1(config)#access-list 1 permit 10.1.1.0 0.0.0.3
R1(config)#route-map Leak-Route permit 10 // this command will also remove the "route_map Leak-Route deny 10" command.
R1(config-route-map)#match ip address 1

NEW QUESTION: 184

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: (SHOW ANSWER)
IPv6 Source Guard uses the IPv6 First-Hop Security Binding Table to drop traffic from unknown sources or bogus IPv6 addresses not in the binding table. The switch also tries to recover from lost address information, querying DHCPv6 server or using IPv6 neighbor discovery to verify the source IPv6 address after dropping the offending packet(s).
Reference: https://blog.ipspace.net/2013/07/first-hop-ipv6-security-features-in.html

NEW QUESTION: 185

Refer to the exhibit. An engineer cannot determine the time of the problem on R1 due to a mismatch between the router local clock and legs. Which command synchronizes the time between new log entries and the local clock on R1?
A. service timestamps debug datetime msec show.timezone
B. service timestamps datebug datetime localtime msec
C. service timestamps log datetime msec show-timezone
D. service timestamps log datetime locatetime msec
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
Which two technologies optimize MPLS infrastructure using bandwidth protection services when experiencing slow response7 (Choose two.)
A. Fast-Rwoute
B. SO-MPLS
C. IPLFA
D. VPLS
E. MPLS OAM
Answer: (SHOW ANSWER)

NEW QUESTION: 187
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
```

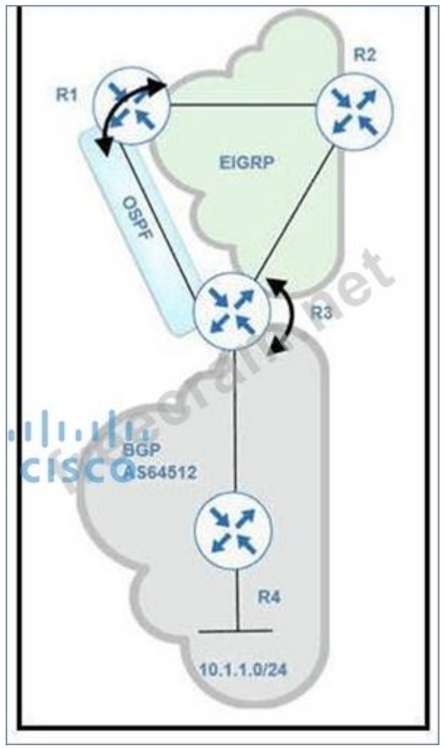
C.
```
router eigrp 100
   redistribute ospf 1 subnets
```

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

Answer: B (LEAVE A REPLY)
"LA router receives all the NewYork routes but it does not receive any LA routes" because when redistrubuting into EIGRP, we must configure the default metric.

NEW QUESTION: 188
Which IPv6 first hop security feature controls the traffic necessary for proper discovery of neighbor device operation and performance?
A. IPv6 Snooping
B. RA Throttling
C. Source or Destination Guard
D. ND Multicast Suppression
Answer: (SHOW ANSWER)

NEW QUESTION: 189
Refer to the exhibit.

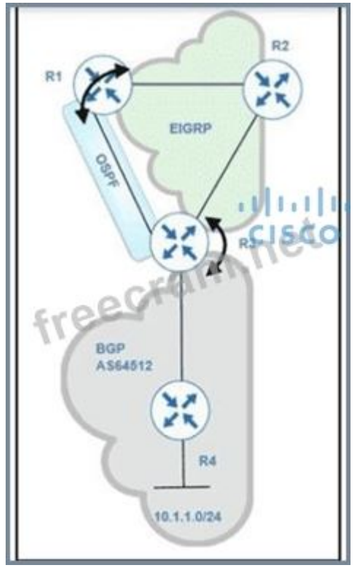


BGP and EIGRP are mutually redistributed on R3, and EIGRP and OSPF are mutually redistributed on R1.
Users report packet loss and interruption of service to applications hosted onthe 10.1.1.0724 prefix. An engineer tested the link from R3 to R4 with no packet loss present but has noticed frequent routing 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. 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.
C. Place an OSPF distribute-list outbound on R3 to block the 10.1.10/24 prefix from being advertised back to R3.
D. Reduce frequent OSPF SPF calculations on R3 that cause a high CPU and packet loss on traffic traversing R3.
Answer: (SHOW ANSWER)
After redistribution, R3 learns about network 10.1.1.0/24 via two paths:
+ Internal BGP (IBGP): advertised from R4 with AD of 200 (and metric of 0)
+ OSPF: advertised from R1 with AD of 110 (O E2) (and metric of 20)
Therefore R3 will choose the path with the lower AD via OSPF
But this is a looped path which is received from R3 -> R2 -> R1 -> R3. So when the advertised route from R4 is expired, the looped path is also expired soon and R3 will reinstall the main path from R4.
This is the cause of intermittent connectivity.
We can solve this problem by denying the 10.1.1.0/24 prefix from being redistributed into OSPF on R1. So R3 will not learn this prefix from R1.
Or another solution is to place an OSPF distribute-list inbound on R3 to block the 10.1.1.0/24 prefix from being advertised back to R3.

NEW QUESTION: 190
What is a limitation of IPv6 RA Guard?
A. It is not supported in hardware when TCAM is programmed

B. It does not offer protection in environments where IPv6 traffic is tunneled.
C. It cannot be configured on a switch port interface in the ingress direction
D. Packets that are dropped by IPv6 RA Guard cannot be spanned
Answer: (SHOW ANSWER)
Restrictions for IPv6 RA Guard
The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
This feature can be configured on a switch port interface in the ingress direction.
This feature supports host mode and router mode.
This feature is supported only in the ingress direction; it is not supported in the egress direction.
This feature is not supported on EtherChannel and EtherChannel port members.
This feature is not supported on trunk ports with merge mode.
This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
Packets dropped by the IPv6 RA Guard feature can be spanned.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16-10/ip6f-xe-16-10-book
/ip6-ra-guard.html#GUID-589AF00C-7499-439F-AD23-51005D61CAB7

NEW QUESTION: 191
Refer to exhibit.

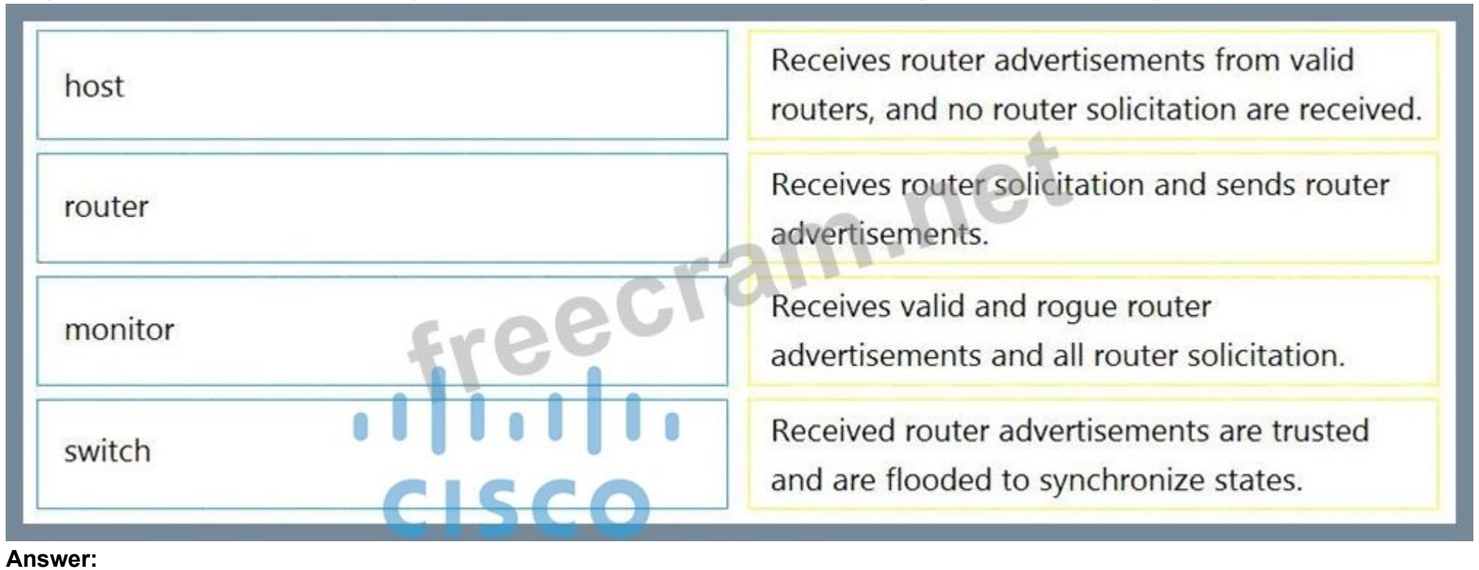


Routing protocols are mutually redistributed on R3 and R1. Users report intermittent connectivity to services hosted on the 10.1.1.0/24 prefix. Significant routing update changes are noticed on R3 when the show ip route profile command is run. How must the services be stabilized?
A. The issue with using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

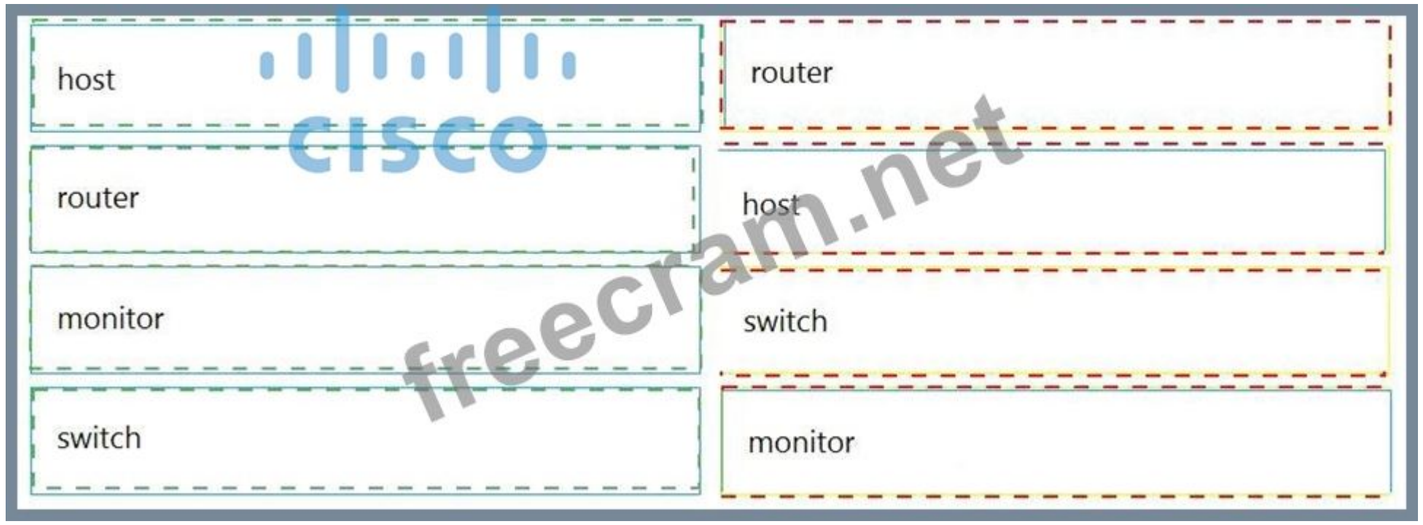
D. The issue with using iBGP must be fixed by running eBGP between R3 and R4
Answer: (SHOW ANSWER)
After redistribution, R3 learns about network 10.1.1.0/24 via two paths:+ Internal BGP (IBGP): advertised from R4 with AD of 200 (and metric of 0)+ OSPF: advertised from R1 with AD of 110 (O E2) (and metric of 20)Therefore R3 will choose the path with the lower AD via OSPF
But this is a looped path which is received from R3 -> R2 -> R1 -> R3. So when the advertised route from R4 is expired, the looped path is also expired soon and R3 willreinstall the main path from R4. This is the cause of intermittent connectivity.In order to solve this issue, we can lower the AD of iBGP to a value which is lower than 110 so that it is preferred over OSPF-advertised route.

NEW QUESTION: 192
Which two protocols work in the control plane of P routers across the MPLS cloud? (choose two)
A. MPLS OAM
B. ECMP
C. RSVP
D. LSP
E. LDP
Answer: (SHOW ANSWER)

NEW QUESTION: 193
Drag and drop the IPv6 first hop security device roles from the left onto the corresponding descriptions on the right.

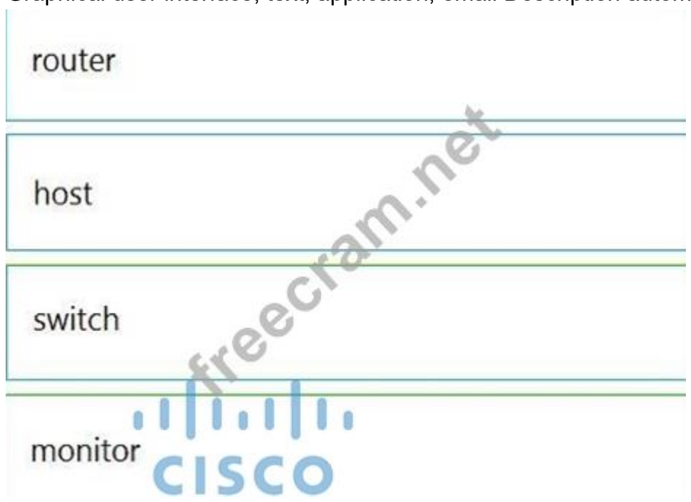


Answer:



Explanation:

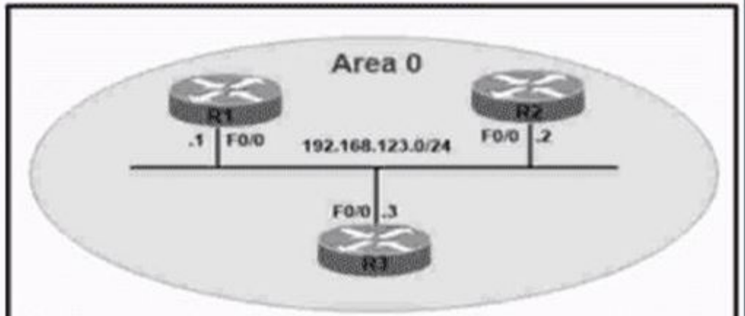
Graphical user interface, text, application, email Description automatically generated



Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX- OS_Security_Configuration_Guide_7x_chapter_011011.pdf

NEW QUESTION: 194



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	00:00:31	192.168.123.1	FastEthernet0/0
192.168.123.3	1	FULL/DR	00:00:32	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	00:00:31	192.168.123.1	FastEthernet0/0
192.168.123.3	1	FULL/DR	00:00:32	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	00:00:36	192.168.123.1	FastEthernet0/0
192.168.123.2	1	FULL/BDR	00:00:39	192.168.123.2	FastEthernet0/0

Refer to the exhibit. 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 FO/0 interface, configure OSPF priority to 201.

B. On the R1 F0/0 interface, configure OSPF priority to 202.

C. On the R2 FO/0 interface, configure OSPF priority to 200.

D. On the R3 FO'O interface, configure OSPF priority to 201.

E. On the R1 FO/0 interface, configure OSPF priority to 255.

Answer: (SHOW ANSWER)

NEW QUESTION: 195

Refer to the exhibit.

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

A. Add a floating static route to the source on R1 to the GigabitEthernet 0/1 interface

B. Modify the uRPF mode from strict to loose

C. Remove the access list from the interface GigabrtEthernet 0/0

D. Enable Cisco Express Forwarding to ensure that uRPF is functioning correctly

Answer: (SHOW ANSWER)

NEW QUESTION: 196

Which mechanism must be chosen to optimize the reconvergence time for OSPF at company location 407173257 that is less CPU-intensive than reducing the hello and dead timers?

A. Dead Peer Detection keepalives

B. BFD

C. SSO

D. OSPF demand circuit

Answer: (SHOW ANSWER)

NEW QUESTION: 197

i.

Which two labet distribution methods are used by routers in MPLS? (Choose two)

A. downstream unsolicited

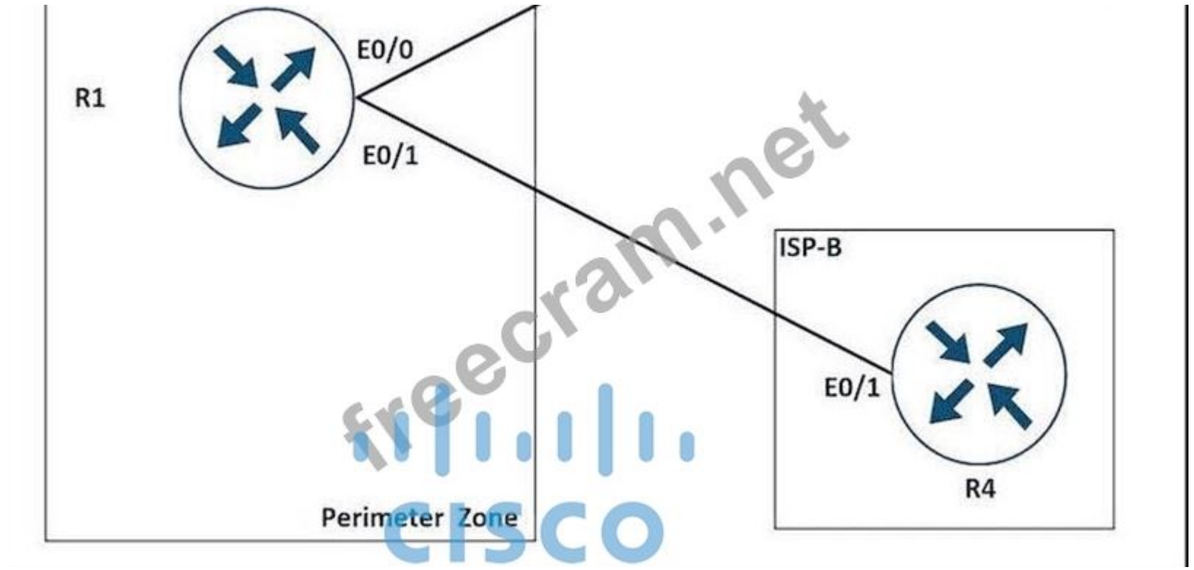
B. LDP discovery hello message

C. downstream on demand

D. LDP session protection message

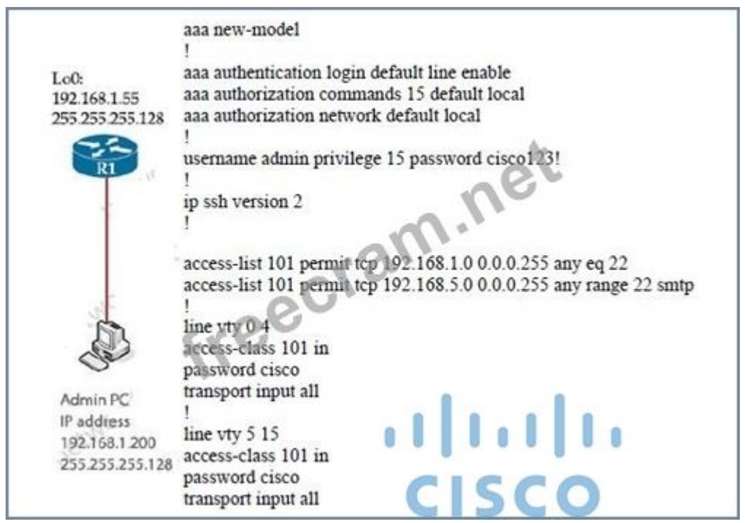
E. targeted hello message
Answer: (SHOW ANSWER)

NEW QUESTION: 198
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. no terminal monitor
B. (config)#terminal no monitor
C. #terminal no monitor
D. (config)#no terminal monitor
Answer: (SHOW ANSWER)
To turn off terminal monitor, use "terminal no monitor" in the enable mode

NEW QUESTION: 199
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. matching password on vty lines as cisco123!

C. enable secret or enable password commands to enter into privileged mode

D. secret cisco123! at the end of the username command instead of password cisco123!

Answer: (SHOW ANSWER)

NEW QUESTION: 200

A customer is running an mGRE DMVPN tunnel over WAN infrastructure between hub and spoke sites. The existing configuration allows NHRP to add spoke routers automatically to the multicast NHRP mappings. The customer is migrated the network from IPv4 to the IPv6 addressing scheme for those spokes' routers that support IPv6 and can run DMVPN tunnel over the IPv6 network. Which configuration must be applied to support IPv4 and IPv6 DMVPN tunnel on spoke routers?

A. Tunnel mode ipv6ip 6rd

B. Tunnel mode ipv6ip isatap

C. Tunnel mode ipv6ip auto-tunnel

D. Tunnel mode ipv6ip 6to4

Answer: (SHOW ANSWER)

NEW QUESTION: 201

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, 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#|
```

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?

A. Use a prefix list instead of an access list in the route map.

B. Use an extended access list instead of a standard access list.

C. Change sequence 10 in the route-map command from permit to deny.

D. Add this statement to the route map: route-map RM-OSPF-DL deny 20.

Answer: (SHOW ANSWER)

NEW QUESTION: 202

Refer to the exhibit.

```
R1#show ip ssh
SSH Disabled – version 1.99
%Please create RSA keys to enable SSH (and of atleast 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#
```

An engineer is trying to connect to a device with SSH but cannot connect. The engineer connects by using the console and finds the displayed output when troubleshooting. Which command must be used in configuration mode to enable SSH on the device?

A. no ip ssh disable

B. ip ssh enable

C. ip ssh version 2

D. crypto key generate rsa

Answer: (SHOW ANSWER)

NEW QUESTION: 203

What is a function of the IPv6 DHCP Guard feature for DHCP messages?

A. It blocks only DHCP request messages.
B. All client messages are always switched regardless of the device role.
C. If the device is configured as a DHCP server, no message is switched.
D. Only access lists are supported for matching traffic.
Answer: (SHOW ANSWER)

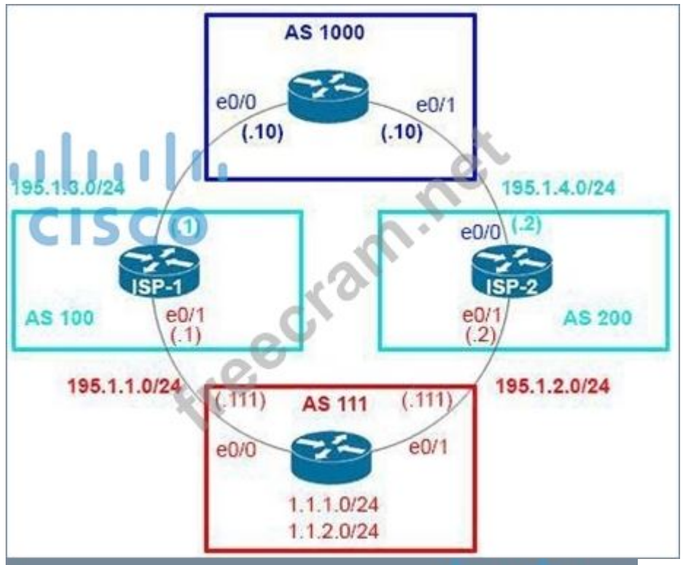
NEW QUESTION: 204
Which command allows traffic to load-balance in an MPLS Layer 3 VPN configuration?
A. multi-paths eibgp 2
B. maximum-paths 2
C. Maximum-paths ibgp 2
D. multi-paths 2
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mpls_cg/mp_vpn_multipath.html

NEW QUESTION: 205

```
*Sep 3 23:18:21.264: EIGRP: Neighbor (10.1.2.192) not yet found
*Sep 3 23:19:18.675: Going down: Peer 10.1.2.1 total=2 stub 0, iidb-stub=0 iid-all=0
*Sep 3 23:19:18.675: EIGRP: Handle deallocation failure [1]
*Sep 3 23:19:18.675: EIGRP: Neighbor 10.1.2.1 went down on Tunnel1.
*Sep 3 23:19:22.943: EIGRP: New peer 10.1.2.1
*Sep 3 23:19:22.943: %DUAL-5-NBRCHANGE: EIGRP-IPv4 3111: Neighbor 10.1.2.1 (Tunnel1) is up: new adjacency
```

Refer to the exhibit. Which configuration command establishes an EIGRP neighbor adjacency between the hub and spoke?
A. eigrp-peer 10.1.2.192 command on the hub router
B. neighbor 10.1.2.192 command on hub router
C. connected 10.1.2.192 command on spoke router
D. network 10.1.2.192 command on spoke router
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Refer to the exhibit.



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

A.
```
router bgp 111
 neighbor 195.1.1.1 as-override
 neighbor 195.1.2.2 as-override
```

B.
```
router bgp 111
 neighbor 195.1.1.1 as-override
 no neighbor 195.1.2.2 allowas-in
```

C.
```
router bgp 111
 no neighbor 195.1.1.1 allowas-in
 no neighbor 195.1.2.2 allowas-in
```

D.
```
router bgp 111
 neighbor 195.1.2.2 as-override
 no neighbor 195.1.1.1 allowas-in
```

Answer: C (LEAVE A REPLY)

A router discards BGP network prefixes if it sees its ASN in AS-Path as a loop prevention mechanism. The "allowas-in" feature allows routes to be received and processed even if router detects its own ASN in AS-Path.

NEW QUESTION: 207

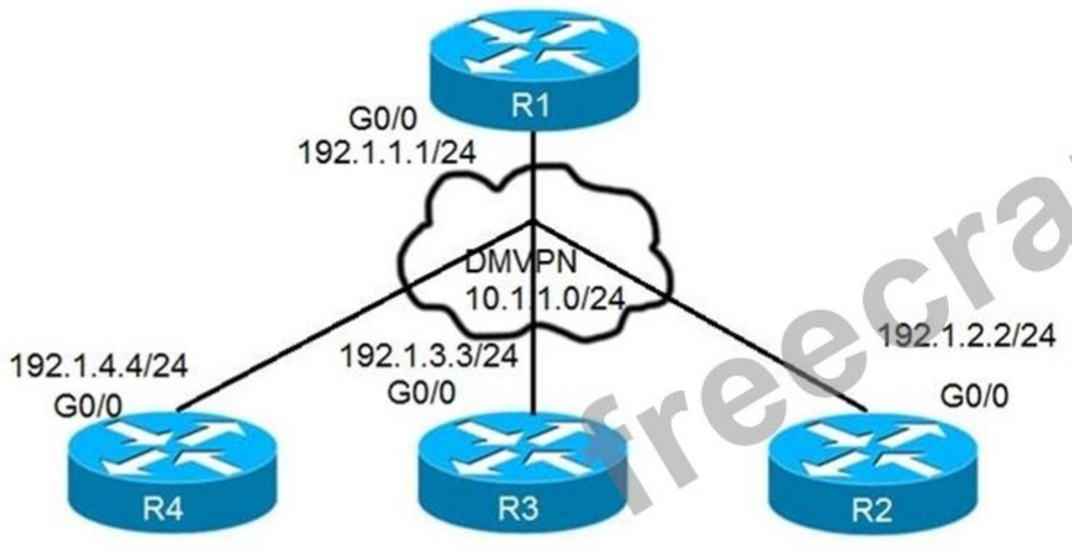
An engineer configured a router with this configuration

ip access-hst 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 tcp
192.168.1.10(1022)(FastEthernet1/0 D508.89gb.003f) ->192.168.2.20(23), 1 packet" Which action stops messages on the console while still denying Telnet?
A. Replace log-input keyword with the log keyword in the access list.
B. Configure a 20 permit ip any any command
C. Configure a 20 permit ip any any log-input command.
D. Remove log-Input keyword from the access list.
Answer: (SHOW ANSWER)

NEW QUESTION: 208
What is a role of route distinguishers in an MPLS network?
A. Route distinguishers define which prefixes are imported and exported on the edge router
B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
C. Route distinguishers make a unique VPNv4 address across the MPLS network
D. Route distinguishers are used for label bindings.
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Which two components are needed for a service provider to utilize the LVPN MPLS application? (Choose two.)
A. The P routers must be configured for MP-iBGP toward the PE routers
B. The P routers must be configured with RSVP.
C. The PE routers must be configured for MP-iBGP with other PE routers
D. The PE routers must be configured for MP-eBGP to connect to CEs
E. The P and PE routers must be configured with LDP or RSVP
Answer: (SHOW ANSWER)
MPLS Network Protocols
+ IGP: OSPF, EIGRP, IS-IS on core facing and core links+ RSVP and/or LDP on core and/or core facing links ->
+ MP-iBGP on PE devices (for MPLS services), MP-BGP: Multiprotocol Border Gateway Protocol, used for MPLS L3 VPN -> .
Reference: https://www.uio.no/studier/emner/matnat/ifi/IN3230/h19/kursmateriell/mpls-lecture.pdf

NEW QUESTION: 210
Refer to the exhibit.



on 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-md-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

on 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

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 resolve the issue? (Choose two.)

A. Configure the crypto isakmp key cisco address 192.1.1.1 on R2 and R3

B. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3.

C. Change the mode from mode tunnel to mode transport on R3

D. Change the mode from mode transport to mode tunnel on R2.

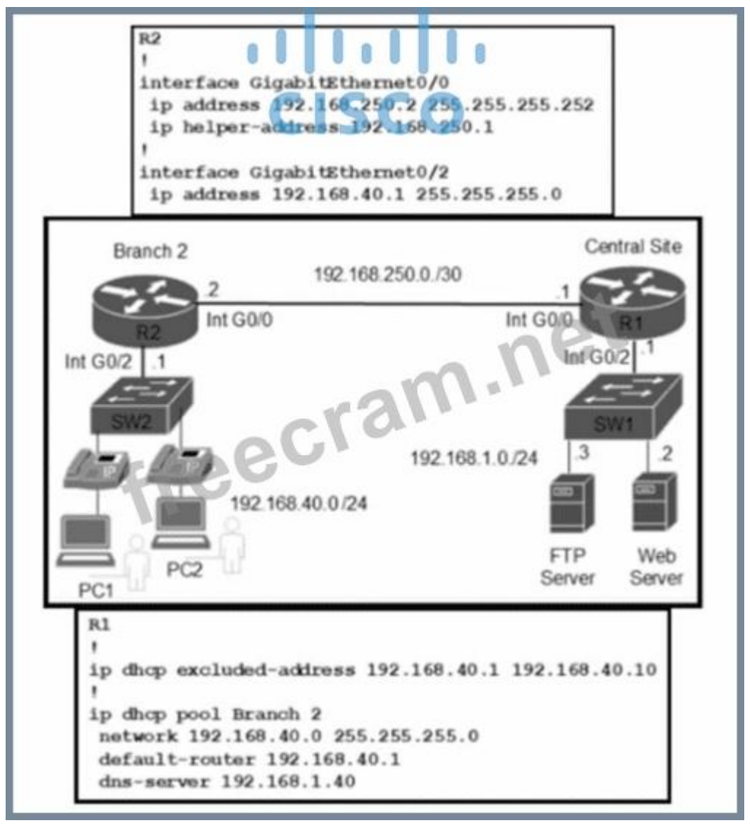
E. Remove the crypto isakmp key cisco address 10.1.1.1 on R2 and R3

Answer: (SHOW ANSWER)

*When using DMVPN with IPSec, it is unnecessary to use tunnel mode. Because DMVPN uses GRE which means that a new IP header is already added by GRE. The GRE encapsulation happens on the tunnel interface before the encryption process takes place.

NEW QUESTION: 211

:582



Refer to the exhibit. Branch 2 hosts cannot receive dynamic IP addresses. Which action resolves the issue?

A. Configure the ip helper command on the interface GigabitEthernet 0/2 of the R2 router

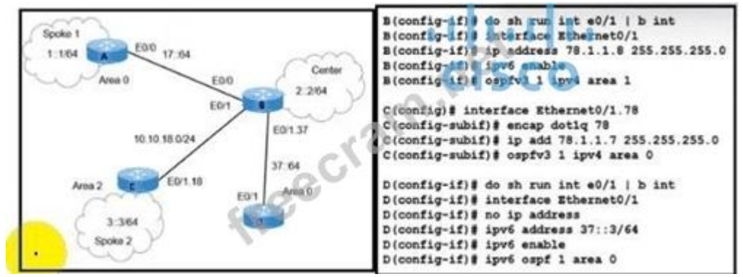
B. Configure the Ip helper command on the Layer 2 switch SW2 interfaces

C. Configure the Ip helper command on the interface GigabitEthernet 0/0 of the DHCP router.

D. Configure the Ip helper command on the interface GigabitEthernet 0/2 of the DHCP router.

Answer: (SHOW ANSWER)

NEW QUESTION: 212



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 OSPFv2 on the routers B and C interfaces

B. Configure IPv6 on the routers B and C interfaces

C. Configure the Spoke 2 users IP on the router B OSPF domain

D. Configure encapsulation dot1q 78 on the router C interface.

Answer: (SHOW ANSWER)

NEW QUESTION: 213

Which statement about route distinguishers in an MPLS network is true?

A. Route distinguishers are used for label bindings.

B. Route distinguishers define which prefixes are imported and exported on the edge router.

C. Route distinguishers make a unique VPNv4 address across the MPLS network.

D. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.

Answer: (SHOW ANSWER)

NEW QUESTION: 214

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.

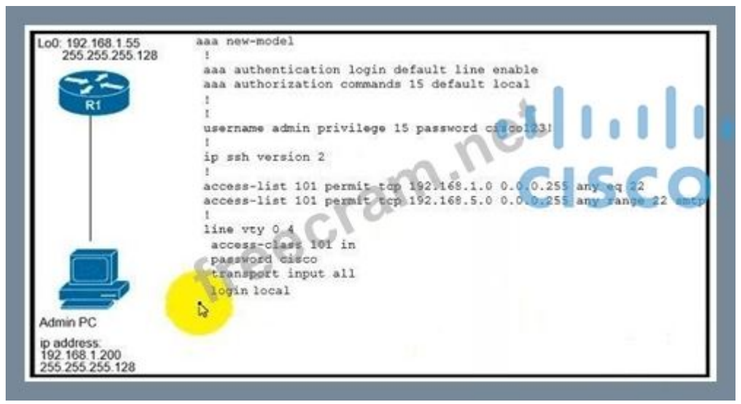
Answer: (SHOW ANSWER)

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents.

Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes).

If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

NEW QUESTION: 215



Refer to the exhibit. 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 authorization exec default local

B. aaa authentication login default local

C. aaa authorization network default local

D. aaa authentication login default enable

Answer: (SHOW ANSWER)

NEW QUESTION: 216

What is the purpose of an OSPF sham-link?

A. to correct OSPF backdoor routing when OSPF is used as the PE-PE connection protocol m an MPLS VPN network

B. to allow intra-area routing when OSPF is used as the PE-CE connection protocol in an MPLS VPN network

C. to correct OSPF backdoor routing when OSPF is used as the PE-CE connection protocol *i an MPLS VPN network

D. to allow inter-area routing when OSPF is used as the PE-CE connection protocol in a MPLS VPN network

Answer: (SHOW ANSWER)

NEW QUESTION: 217

Refer to Exhibit.

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

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

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

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

Answer: (SHOW ANSWER)

A DHCP server that receives a DHCPDISCOVER message may respond with a DHCPOFFER message on UDP port 68 (BootP client).

...

In the event that the DHCP server is not on the local subnet, the DHCP server will send the DHCPOFFER, as a unicast packet, on UDP port 67, back to the DHCP/BootPRelay Agent from which the DHCPDISCOVER came.

Reference: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.

html

NEW QUESTION: 218

Refer to the exhibit.

R2 is a route reflector, and R1 and R3 are route reflector clients. The route reflector 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?

A. R2 does not have a route to the next hop, so R2 does not advertise the prefix to other clients.

B. In route reflector setups, prefixes are not advertised from one client to another.

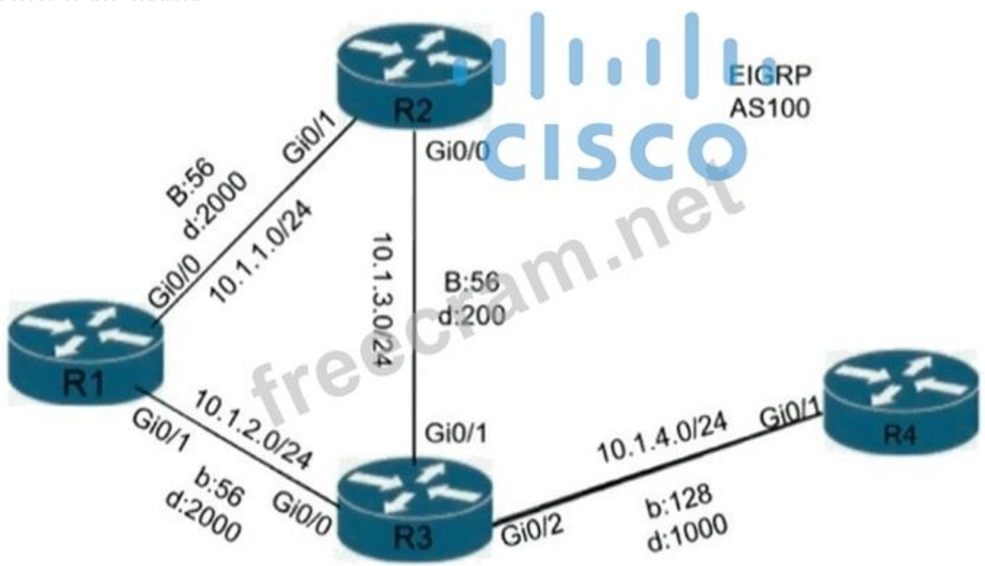
C. Route reflector setup requires full IBGP mesh between the routers.

D. In route reflector setup, only classful prefixes are advertised to other clients.

Answer: (SHOW ANSWER)

NEW QUESTION: 219
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 source port for the SSH connection to initiate
B. Configure a TACACS+ server and enable it
C. Configure transport input ssh command on the console
D. Configure a domain name
E. Configure a crypto key to be generated
Answer: (SHOW ANSWER)
Follow these guidelines when configuring the switch as an SSH server or SSH client:
+ An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.+ If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master
+ If you get CLI error messages after entering the crypto key generate rsa global configuration command, an RSA key pair has not been generated. Reconfigure thehostname and domain, and then enter the crypto key generate rsa command.+ When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the hostname globalconfiguration command.+ When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the ip domain-nameglobal configuration command.+ When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.
Reference:https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook
/configuration_guide/b_consolidated_config_guide_3850_chapter_01100

NEW QUESTION: 220
Refer to the exhibit.



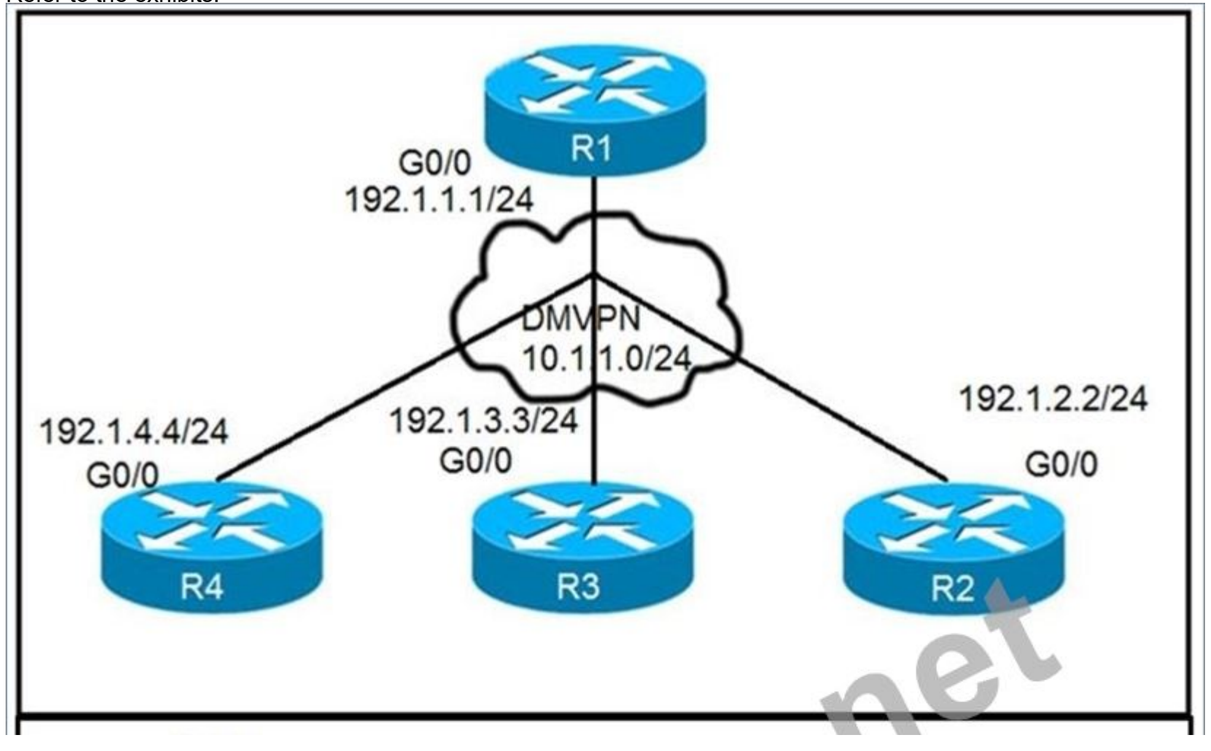
A loop occurs between R1, R2, and R3 while EIGRP is run with poison reverse enabled. Which action prevents the loop between R1, R2, and R3?
A. Configure route filtering
B. Configure route tagging
C. Configure R2 as stub receive-only

D. Enable split horizon
Answer: (SHOW ANSWER)

NEW QUESTION: 221

Refer to the exhibit. An engineer configured SNMP traps to record spoofed packets drop of more than 48000 a minute on the ethernet0/0 interlace. 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 80
B. ip verity unicast notification threshold 48000
C. ip verify unicast notification threshold 800
D. ip verify unicast notification threshold 8000
Answer: (SHOW ANSWER)

NEW QUESTION: 222
Refer to the exhibits.



```
On R1:
R1(config)# interface tunnel 1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source 192.1.1.1
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# ip nhrp network-id 111

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-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

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-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

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 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
```

Phase-3 tunnels cannot be established between spoke-to-spoke in DMVPN. Which two commands are missing? (Choose two.)

A. The ip nhrp redirect command is missing on the spoke routers.

B. The ip nhrp map command is missing on the hub router.

C. The ip nhrp redirect commands is missing on the hub router.

D. The ip nhrp shortcut commands is missing on the hub router.

E. The ip nhrp shortcut command is missing on the spoke routers.

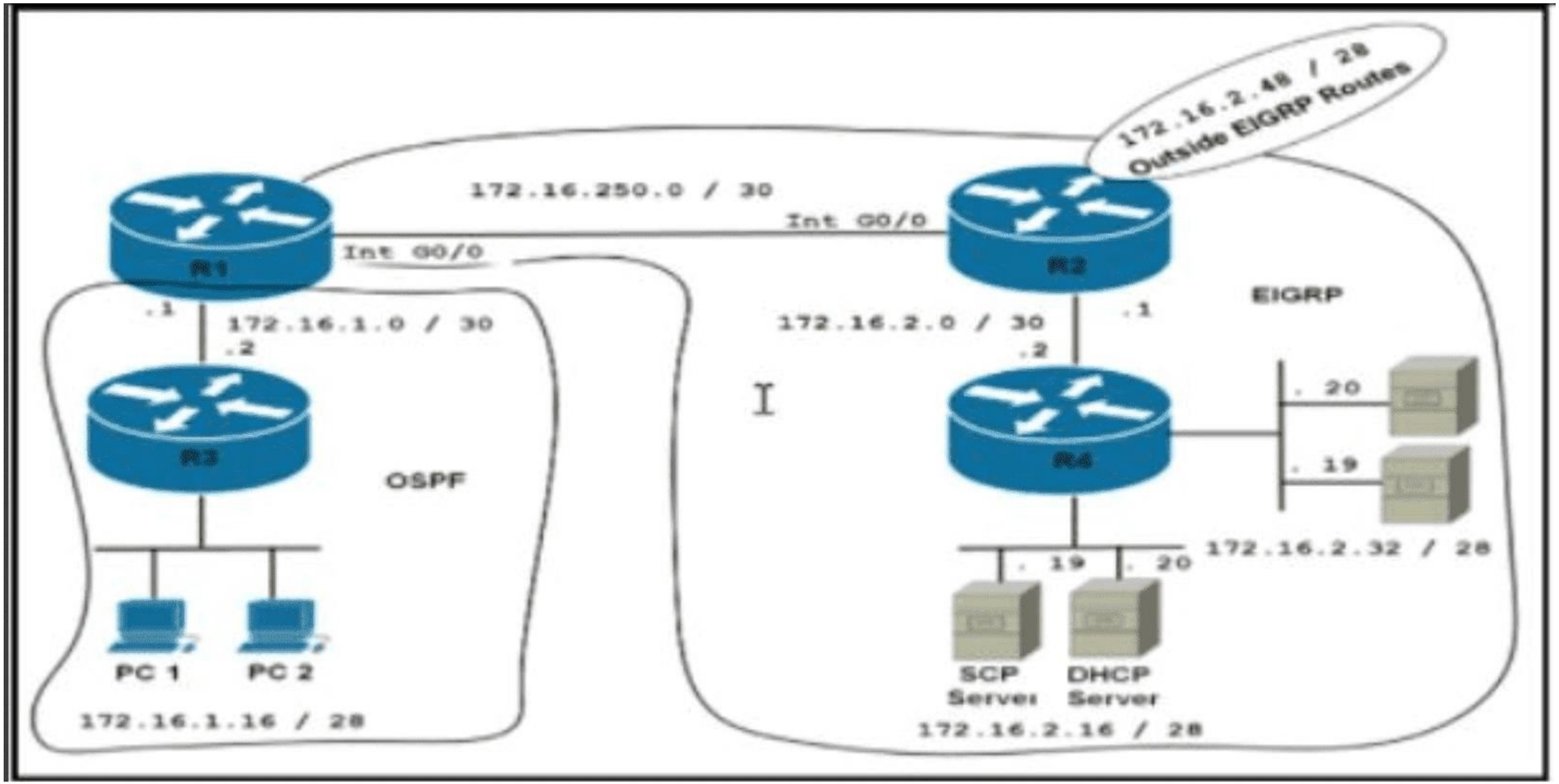
Answer: (SHOW ANSWER)

NEW QUESTION: 223

```
R1#show running-config | begin router eigrp
router eigrp 100
 network 172.16.250.0 0.0.0.3
 redistribute ospf 10 metric 1 1 1 1 1
!
router ospf 10
 redistribute eigrp 100 metric 100 subnets route-map CCNP
 network 172.16.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
route-map CCNP deny 10
 match route-type local
!
!
access-list 10 permit 172.16.2.32
!
```

```
R4#show running-config | begin router eigrp
router eigrp 100
 network 172.16.2.0 0.0.0.3
 network 172.16.2.16 0.0.0.15
 network 172.16.2.32 0.0.0.15
 redistribute static metric 100 1 1 1 1 route-map CCNP
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 172.16.2.48 255.255.255.240 172.16.2.1
!
!
route-map CCNP permit 10
 match ip address 10
 set tag 200
!
!
access-list 10 permit 172.16.2.48 0.0.0.15
!
```

```
R3#sh ip route

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet0/1
L        172.16.1.2/32 is directly connected, GigabitEthernet0/1
C        172.16.1.16/28 is directly connected, Loopback1
L        172.16.1.17/32 is directly connected, Loopback1
C        172.16.1.32/28 is directly connected, Loopback2
L        172.16.1.33/32 is directly connected, Loopback2
S        172.16.1.48/28 [1/0] via 172.16.1.18
R3#
```



Refer to the exhibit. Which configuration resolves the route filtering issue on R1 to redistribute all the routes except 172.16.2.48/28?

A.

```
R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)#match route-type external  type-1
R1(config)#route-map CCNP permit 20
```

B.
```
R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)#match route-type external
R1(config)#route-map CCNP permit 20
```

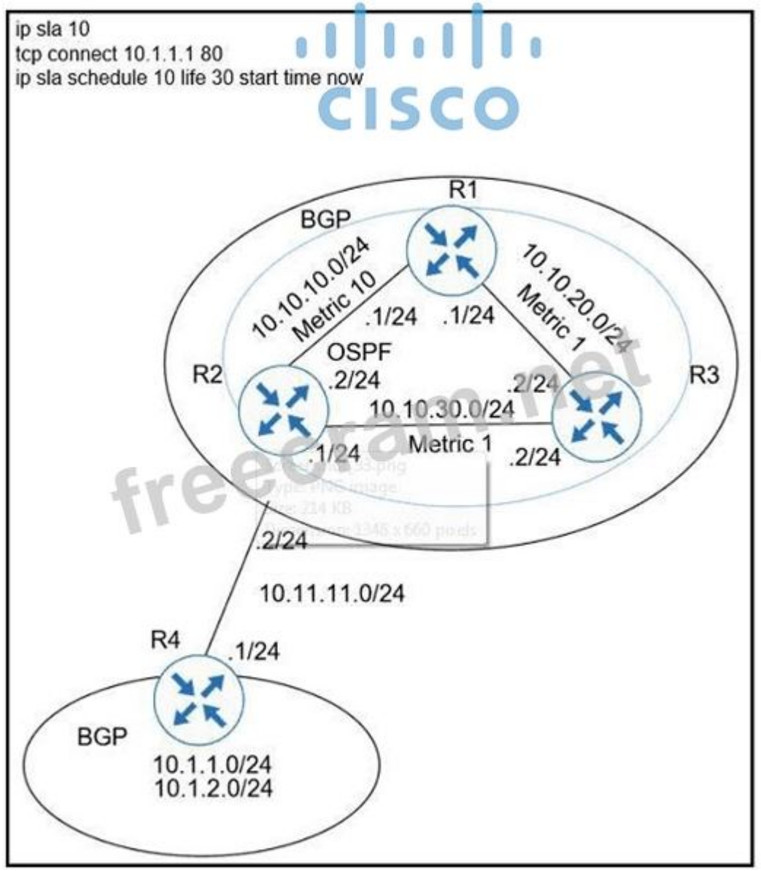
C.
```
R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)# match route-type level-2
R1(config)#route-map CCNP permit 20
```

D.
```
R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)#match route-type external  type-2
R1(config)#route-map CCNP permit 20
```

Answer: (SHOW ANSWER)

NEW QUESTION: 224

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: (SHOW ANSWER)

NEW QUESTION: 225

Which Layer 3 VPN attribute installs customer routes in the VRF?

A. extended-community

B. RT

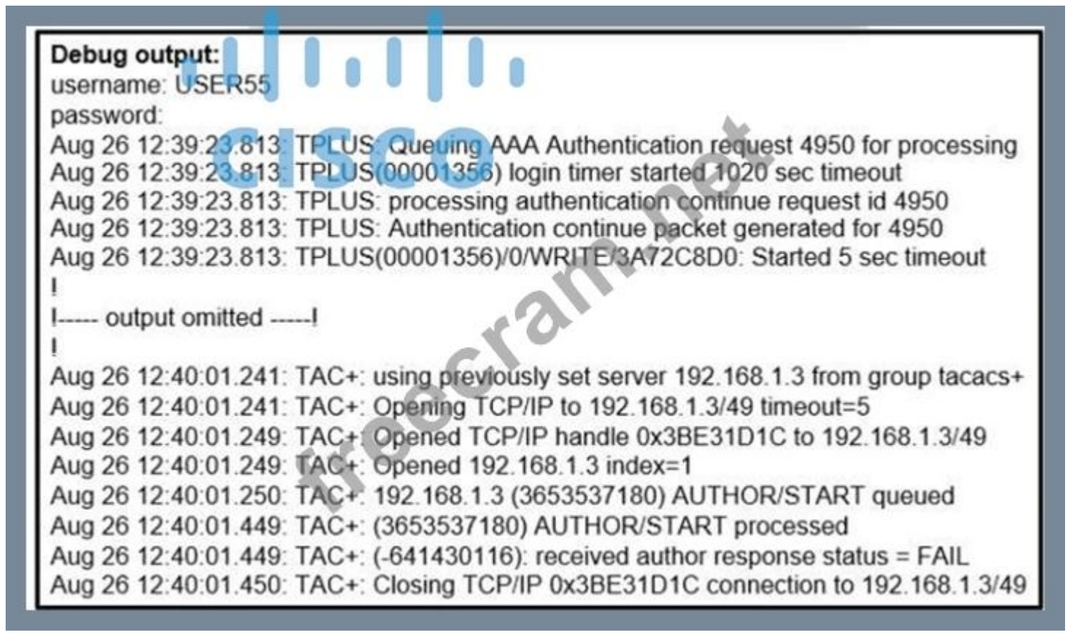
C. RD

D. MPLS label

Answer: (SHOW ANSWER)

NEW QUESTION: 226

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?

A. Configure an authorized IP address for this user to access this router

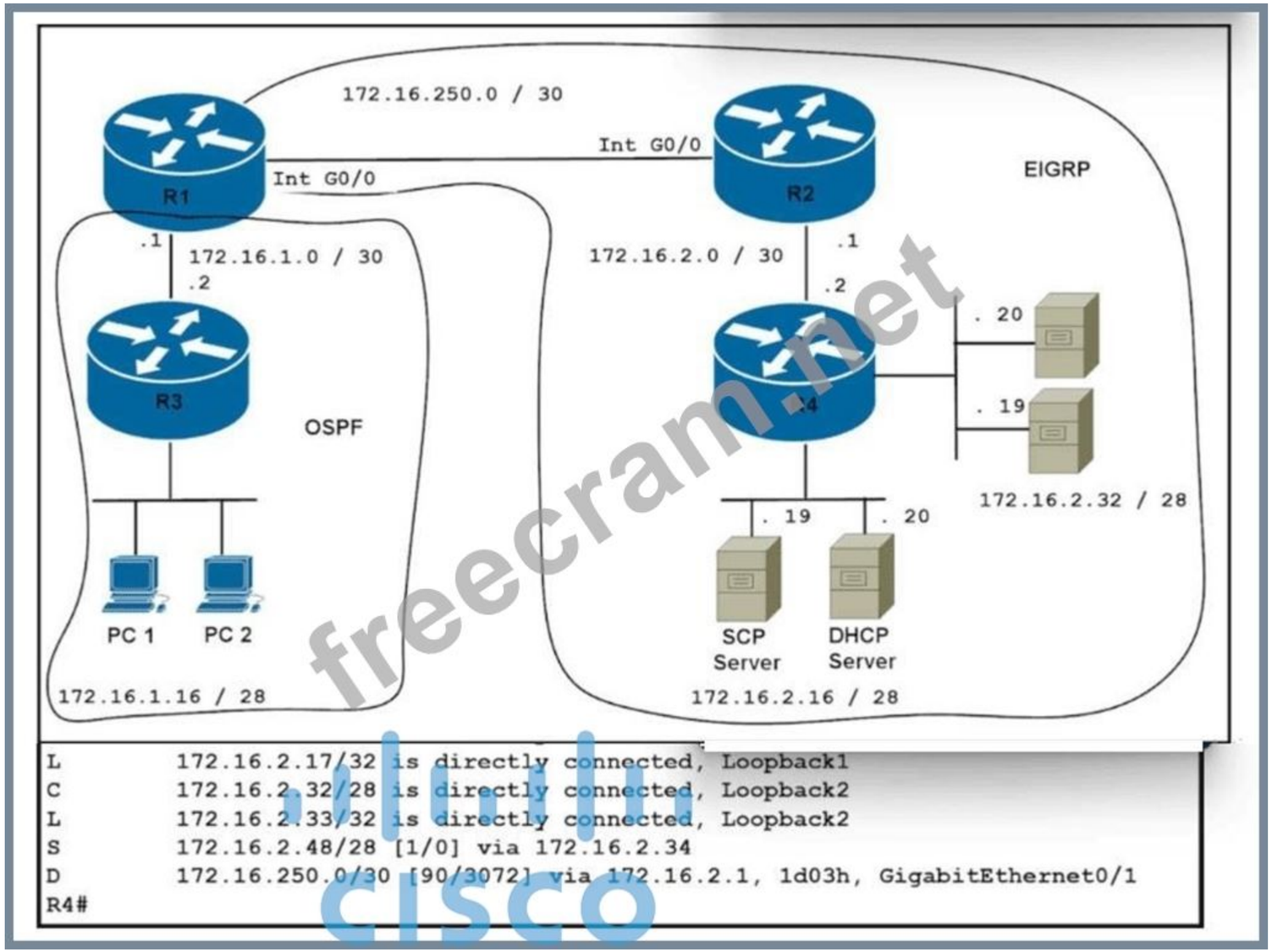
B. Configure full access for the username from TACACS+ server

C. Configure the username from a local database

D. Configure TACACS+ synchronization with the Active Directory admin group

Answer: B (LEAVE A REPLY)

NEW QUESTION: 227



Refer to the exhibit. The users from subnet 172.16.1.16/28 are experiencing connectivity issues to subnet 172.16.2.32/48. Which configuration resolves the issue?

A. R1(config)#route-map REDIST permit 10
R1(config-roule-map) #match ip address 15
R1 (config-route-map) #exlt
R1(config)# access-list 15 permit 172.16.0.0 0.0.255.255
R1(config-router) #router ospf 1
R1(config-router) #redistrlbute elgrp 100 subnets route-map REDIST

B. R1(config)#route-map REDIST permit 10

R1(config-route-map) #match Ip address 15
R1 (config-route-map) #exit
R1(config)# access-list 15 permit 172.16.0.0 0.0.255.255
R1(config-router) #router eigrp 100
R1(config-router) #redistrlbute ospf 1 route-map REDIST
C. R1(config-router>#routereigrp 100
R1(config-router>#redistribute ospf 1 metric 1000000 1111
D. R1(oonfig-router) #router ospf 1
R2(config-router) #redistribute eigrp 100 subnets metric 100C.
Answer: (SHOW ANSWER)

NEW QUESTION: 228

```
R1# configure terminal
R1(config)# hostname CPE1
CPE1(config)# ip domain-name example.com
CPE1(config)# crypto key generate rsa
The name for the keys will be: CPE1.example.com
Choose the size of the key modulus in the range of 360 to 4096
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

CPE1(config)# service password-encryption
CPE1(config)# username csadmin secret Secur3p4s$w0rd
CPE1(config)# line vty 0 4
CPE1(config-line)# transport input telnet ssh
CPE1(config-line)# login local
CPE1(config-line)# end
CPE1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CPE1# ssh 10.0.0.1
% No user specified nor available for SSH client
```

```
CPE1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CPE1# ssh 10.0.0.1
% No user specified nor available for SSH client
```

Refer to the exhibit. An administrator must harden a router, but the administrator failed to test the SSH access successfully to the router. Which action resolves the issue?
A. SSH syntax must be ssh -l user ip to log in to the remote device
B. Configure enable secret to log in to the device
C. SSH must be allowed with the transport output ssh command
D. Configure SSH on the remote device to log m using SSH
Answer: A (LEAVE A REPLY)
NEW QUESTION: 229
Which Layer 3 VPN attribute allows different customers to connect to the same MPLS network wrth overlapping IP ranges?

A. VRF
B. RT
C. MP-BGP
D. RD
Answer: (SHOW ANSWER)
In a Layer 3 VPN (Virtual Private Network) over an MPLS (Multiprotocol Label Switching) network, the attribute that allows different customers to connect with overlapping IP ranges is the Route Distinguisher (RD)
123.
RD is a unique identifier that is prepended to each IP address in a customer's VPN to create a unique VPNv4 address. This allows customers to use overlapping IP addresses without conflict123. The RD makes it possible for the same IP prefix to exist in different VPNs, which is crucial when customers have overlapping IP ranges123.
References:
MPLS Layer 3 VPN Explained - NetworkLessons.com
MPLS: Layer 3 VPNs Configuration Guide - Cisco
Understanding Using MPLS-Based Layer 3 VPNs on Switches - Juniper

NEW QUESTION: 230
Refer to Exhibit.

```
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)
```

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. ip dhcp snooping
B. ip dhcp snooping trust
C. ip dhcp relay information trust portchannel2
D. No ip dhcp snooping information option
Answer: (SHOW ANSWER)

NEW QUESTION: 231
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 though an ACL is configured.

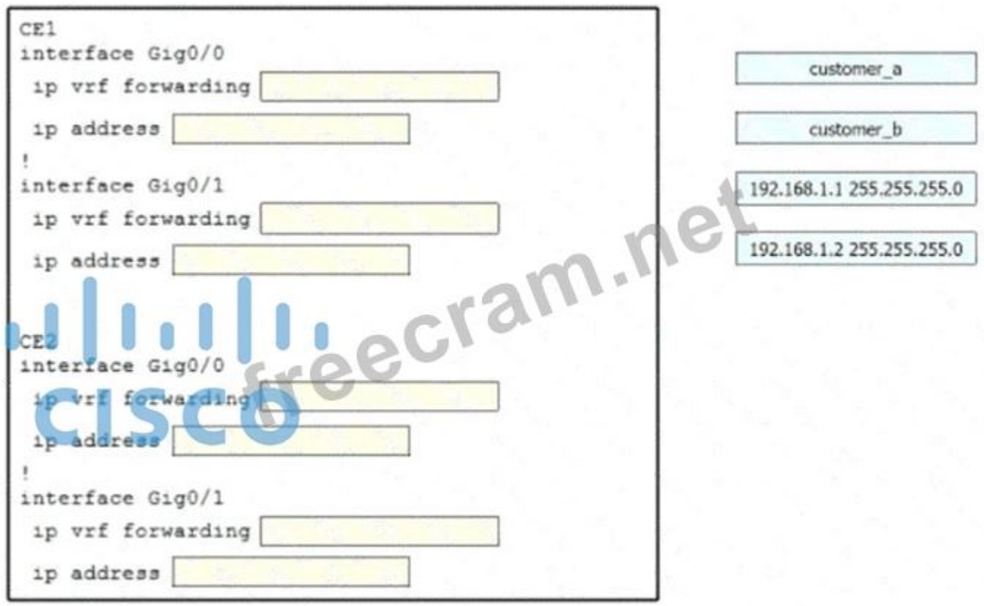
Which command resolves this issue?
A. ip access-group INTERNET in
B. access-class INTERNET in
C. ipv6 access-class INTERNET in
D. ipv6 traffic-filter INTERNET in
Answer: (SHOW ANSWER)

NEW QUESTION: 232
Which command is used to check IP SLA when an interface is suspected to receive lots of traffic with options?
A. show timer
B. show delay
C. show track
D. show threshold
Answer: (SHOW ANSWER)

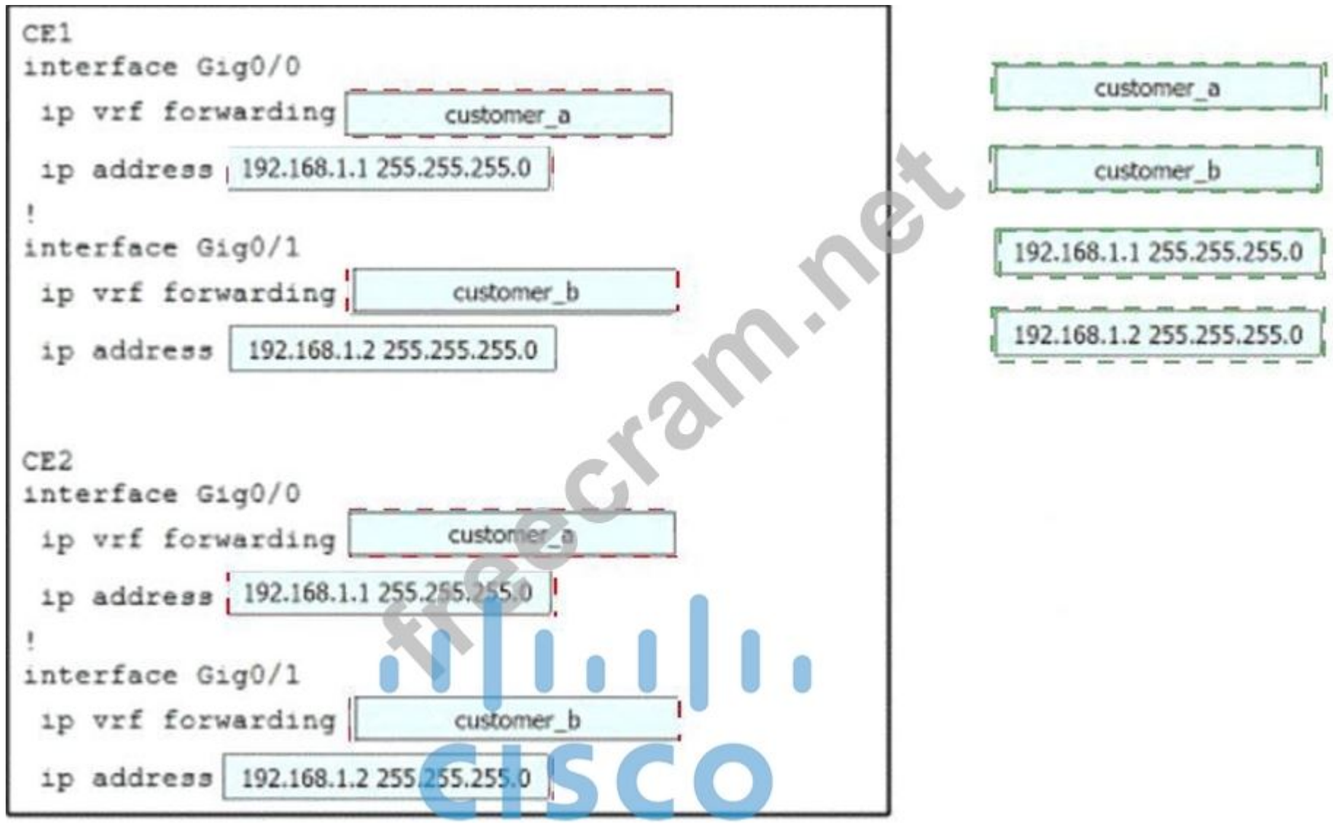
NEW QUESTION: 233
An engineer must establish a connection between two CE routers for two customers with overlapping IP addresses Customer_a is connected to interfaces Gig0/0, and Customer_b is connected to interfaces Gig0/1.
Routers CE1 and CE2 are configured as follows:

```
ip vrf customer_a
 rd 1:1
 route-target both 1:1
!
ip vrf customer_b
 rd 2:2
 route-target both 2:2
```

Drag and drop the code snippets from the right onto the boxes in the configuration to establish the needed connection. Snippets may be used more than once.



Answer:



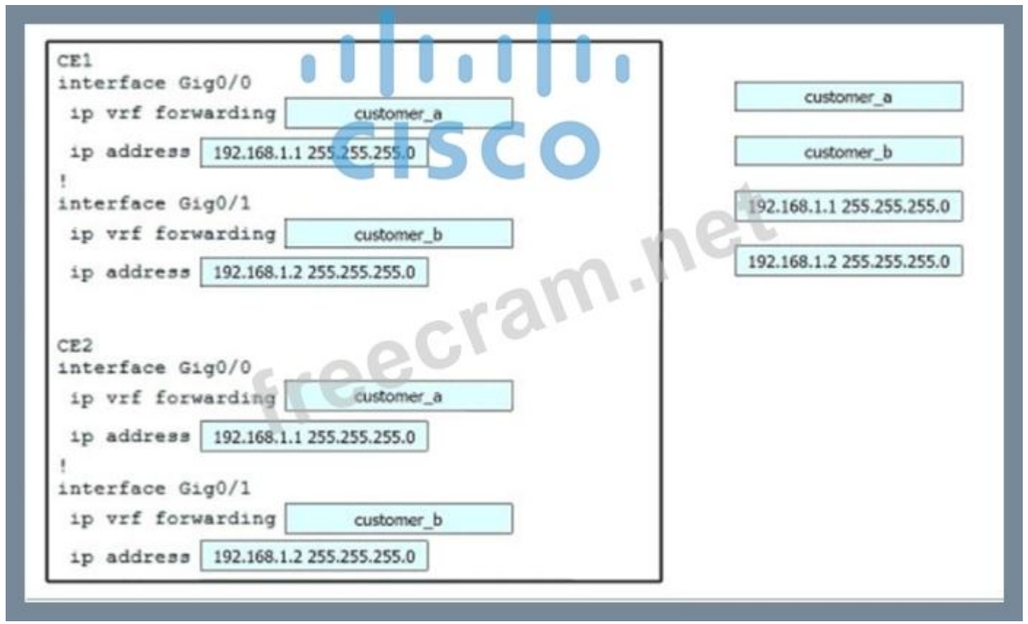
customer_a

customer_b

192.168.1.1 255.255.255.0

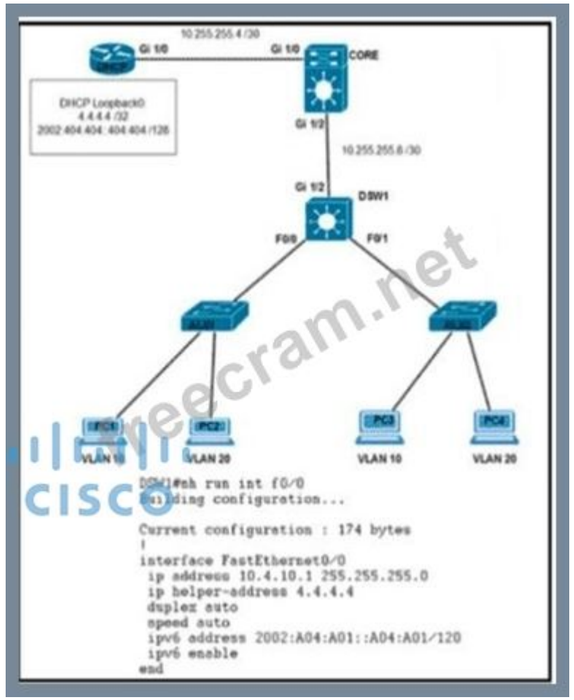
192.168.1.2 255.255.255.0

Explanation:



NEW QUESTION: 234

Clients on ALS2 receive IPv4 and IPv6 addresses but clients on ALS1 receive only IPv4 addresses and not IPv6 addresses. Which action on DSW1 allows clients on ALS1 to receive IPv6 addresses?



A. Configure DSW1(config-if)#ipv6 helper address 2002:404:404::404:404
B. Configure DSW1(dhcp-config)#default-router 2002:A04:A01::A04:A01
C. Configure DSW1(config)#ipv6 route 2002:404:404:404:404/128 FastEthernet1/0
D. Configure DSW1(config-if)#ipv6 dhcp relay destination 2002:404:404::404:404 GigabitEthernet1/2
E. Option A
F. Option B
G. Option C
H. Option B
Answer: (SHOW ANSWER)
https://community.cisco.com/t5/networking-documents/stateful-dhcpv6-relay-configuration-example/ta-p
/3149338

NEW QUESTION: 235
Which two protocols can cause TCP starvation? (Choose two)
A. HTTPS
B. FTP
C. SMTP
D. TFTP
E. SNMP
Answer: (SHOW ANSWER)

NEW QUESTION: 236
Which feature is required for IPv6 Source Guard to block traffic arriving on the server interface from unknown sources?
A. Dynamic ARP Inspection
B. IPv6 RA Guard
C. DHCPv6 Guard
D. IPv6 ND Inspection
Answer: (SHOW ANSWER)

NEW QUESTION: 237
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 o
   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. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF

B. Modify the access list to add a second line of permit ip any

C. Add a sequence 20 in the route map to permit access list 1.

D. Modify distribute list seq 10 to permit the route to 192.168.2.2.

E. Modify the access list to deny the route to 192.168.2.2.

Answer: (SHOW ANSWER)

NEW QUESTION: 238

Which protocol must be secured with MD-5 authentication across the MPLS cloud to prevent hackers from introducing bogus routers?

A. RSVP

B. MP-BGP

C. LDP

D. LSP

Answer: (SHOW ANSWER)

NEW QUESTION: 239

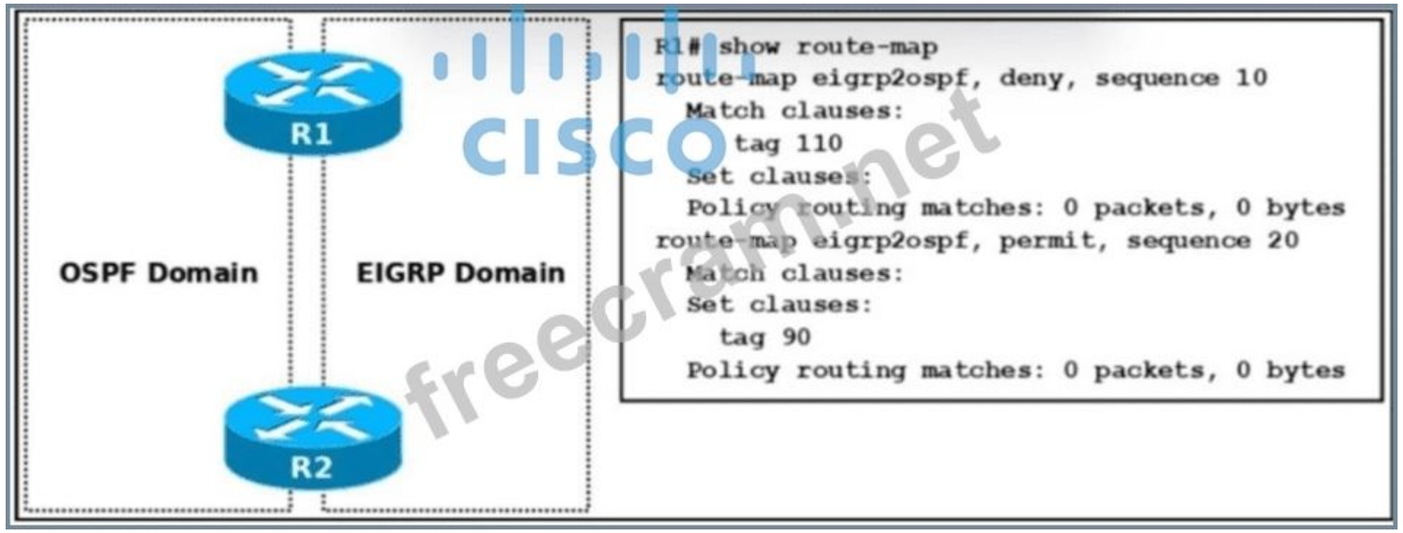
IPv6 is enabled in the infrastructure to support customers with an IPv6 network over WAN and to connect the head office to branch offices in the local network. One of the customers is already running IPv6 and wants to enable IPv6 over the DMVPN network infrastructure between the headend and branch sites.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

A. tunnel protection mode ipv6

B. ipv6 unicast-routing

C. ipv6 nhrp holdtime 30
D. tunnel mode gre multipoint ipv6
Answer: (SHOW ANSWER)
The command "tunnel mode gre multipoint ipv " sets the encapsulation mode of the tunnel to mGRE IPv6.

NEW QUESTION: 240
:593



Refer to the exhibit. Which two configurations are required on R2 to prevent a routing loop caused by the redistribution from OSPF back into EIGRP? (Choose two.)

- [ ] route-map eigrp2ospf permit 10
  set tag 90
  route-map eigrp2ospf deny 20
  match tag 110

- [ ] route-map ospf2eigrp deny 10
  match tag 90
  route-map ospf2eigrp permit 20
  set tag 110

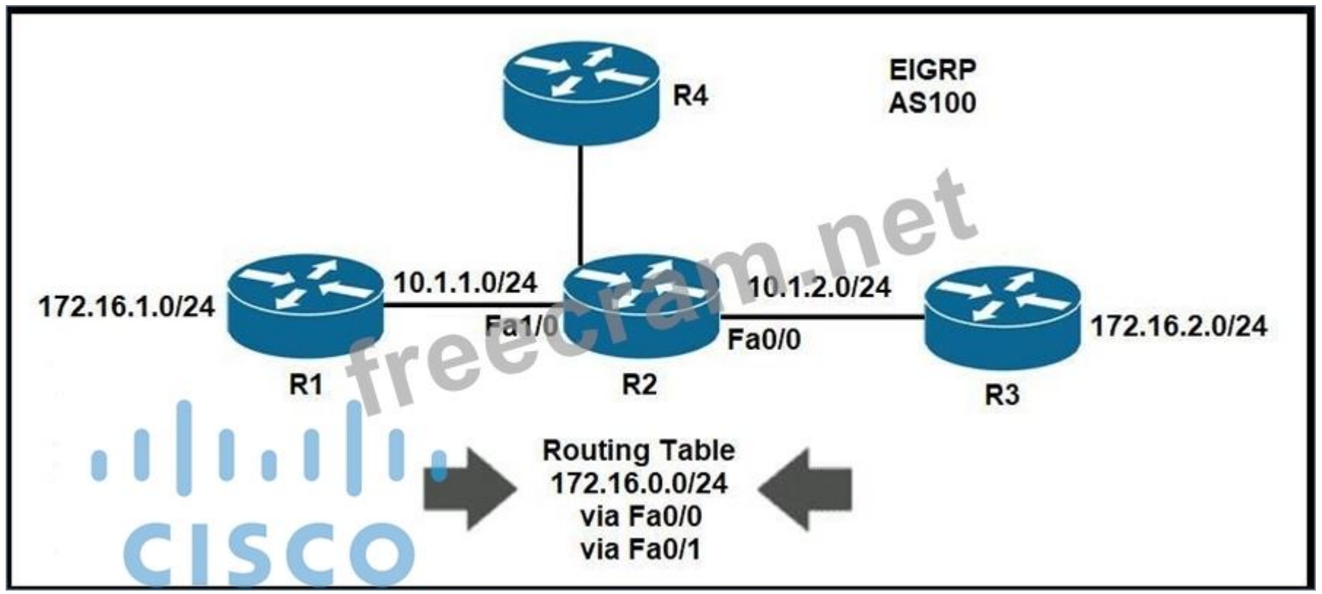
- [ ] router ospf 1
  redistribute eigrp 1 route-map ospf2eigrp

- [ ] router eigrp 1
  redistribute ospf 1 metric 100000 1 255 1 1500 route-map eigrp2ospf

- [ ] router eigrp 1
  redistribute ospf 1 metric 100000 1 255 1 1500 route-map ospf2eigrp

A. Option C
B. Option B
C. Option E
D. Option A
E. Option D
Answer: (SHOW ANSWER)

NEW QUESTION: 241
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. Disable auto summarization on R2

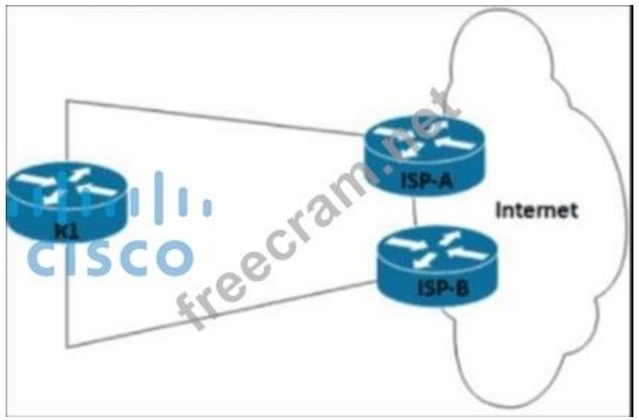
B. Insert a /16 floating static route on R2 toward R3 with metric 254

C. Enable auto summarization on all three routers R1, R2, and R3

D. Insert a /24 floating static route on R2 toward R3 with metric 254

Answer: (SHOW ANSWER)

NEW QUESTION: 242



Refer to the exhibit. Router R1 peers with two ISPs using static routes to get to the internet. The requirement is that R1 must prefer ISP-A under normal circumstances and failover to ISP-B if the connectivity to ISP-A is lost. The engineer observes that R1 is load balancing traffic across the two ISPs Which action resolves the issue by sending traffic to ISP-A only with failover to ISP-B?

A. Configure two static routes on R1. one pointing to ISP-A and another pointing to ISP- B with 222 admin distance

B. Change the bandwidth of the interface on R1 so that interface to ISP-A has a higher value than the interface to ISP-B

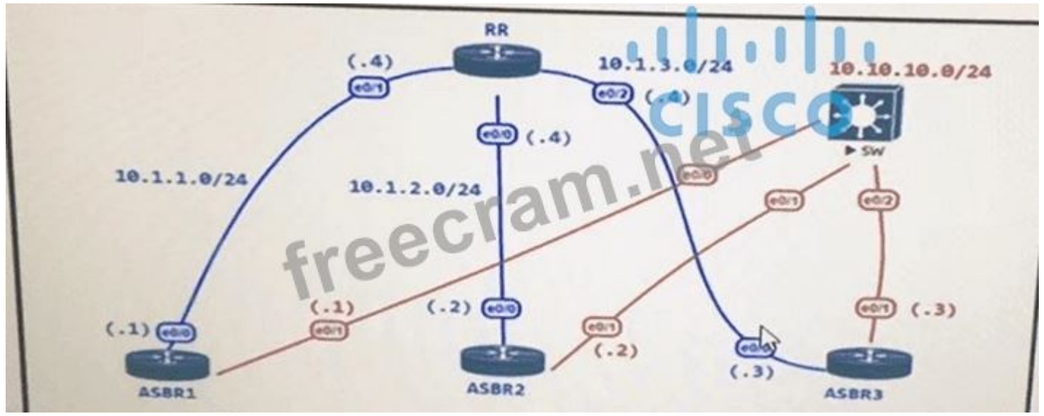
C. Configure OSPF between R1. ISP-A. and ISP-B for dynamic failover if any ISP link to R1 fails

D. Configure two static routes on R1. one pointing to ISP-B with more specific routes and another pointing to ISP-A with summary routes

Answer: (SHOW ANSWER)

NEW QUESTION: 243

Refer to the exhibit.



RR

```
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
```

ASBR2

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

ASBR3

```
router bgp 100
 neighbor 10.1.2.4 remote-as 100
```

ASBR4

```
router bgp 100
 neighbor 10.1.3.4 remote-as 100
```

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

A.
```
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.
```
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
```

C.
```
router bgp 100
 neighbor 10.1.1.1 ebgp-multihop
 neighbor 10.1.2.2 ebgp-multihop
 neighbor 10.1.3.3 ebgp-multihop
```

D.
```
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
```

Answer: (SHOW ANSWER)

NEW QUESTION: 244

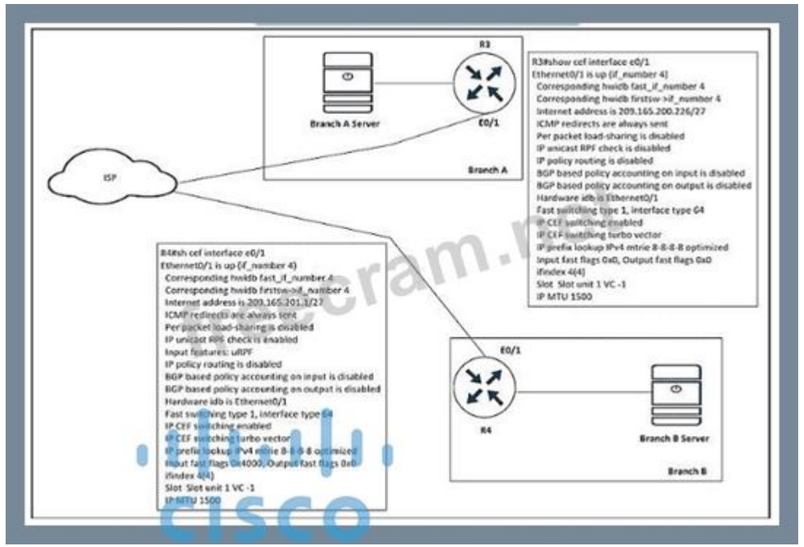
The network administrator configured CoPP so that all SNMP traffic from Cisco Prime located at 192.168.1.11 toward the router CPU is limited to 1000 kbps. Any traffic that exceeds this limit must be dropped.

access-list 100 permit udp any any eq 161

class-map CM-SNMP
match access-group 100
policy-map PM-COPP
class CM-SNMP
police 1000 conform-action transmit
!
control-plane
service-policy input PM-COPP
The network administrator is not getting the desired result for the SNMP traffic and SNMP traffic is getting dropped frequently. Which set of configurations resolves the issue?

A. Option C
B. Option A
C. Option D
D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 245



Refer to the exhibit.

A shoe retail company implemented the uRPF solution for an antispoofing attack. A network engineer received the call that the branch A server is under an IP spoofing attack. Which configuration must be implemented to resolve the attack?

A.
```
R3
interface ethernet0/1
 ip unicast RPF check reachable-via any allow-default allow-self-ping
```

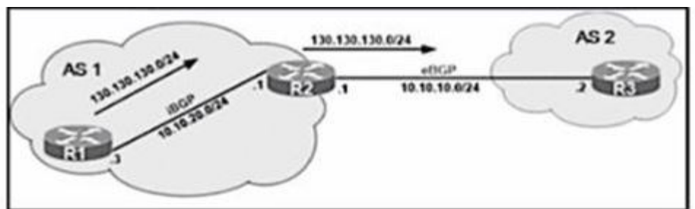
B.
```
R4
interface ethernet0/1
 ip verify unicast source reachable-via any allow-default allow-self-ping
```

C.
```
R4
interface ethernet0/1
  ip unicast RPF check reachable-via any allow-default allow-self-ping
```

D.
```
R3
interface ethernet0/1
 ip verify unicast source reachable-via any allow-default allow-self-ping
```

Answer: (SHOW ANSWER)

NEW QUESTION: 246




```
R2# show ip bgp 130.130.130 255.255.255.0 longer
BGP table version is 4, local router ID is 10.10.20.1

Network          Next Hop    Metric LocPrf Weight Path
* i130.130.130.0/24  10.10.20.3       0    100      0 i

R2# show ip protocols
Routing Protocol is "bgp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
IGP synchronization is enabled
Automatic route summarization is disabled
Neighbor(s):
Address
10.10.10.2
10.10.20.3
Maximum path: 1
Routing for Networks:
Routing Information Sources:
Gateway Distance Last Update
10.10.20.3 200 01:48:24
Distance: external 20 internal 200 local 200
```


Refer to the exhibit. The 130.130.130.0/24 route shows in the R2 routing table but is getting filtering toward R3. Which action resolves the issue?

A. IGP synchronization must be disabled on R2.
B. The incoming filter list for all interfaces must be set on R2.
C. Automatic route summarization must be enabled on R2.
D. The outgoing filter list for all interfaces must be set on R2.
Answer: (SHOW ANSWER)

NEW QUESTION: 247

```
Router A
line con 0
   exec-timeout 60 0
   logout-warning 15
   logging synchronous
   login
   transport output all
   stopbits 1
```

Refer to the exhibit After a misconfiguration by a junior engineer, the console access to router A is not working Which configuration allows access to router A?

A)

```
RouterA(config)#aaa new-model
RouterA(config)#aaa authentication login my-auth-list tacacs+
```

B)

```
RouterA(config)#line console 0
RouterA(config-line)#password cisco
RouterA(config)#end
```

C)

```
RouterA(config)#line console 0
RouterA(config-line)#password cisco
RouterA(config-line)#login local
RouterA(config)#end
```

D)

A. Option A

B. Option B

C. Option C

D. Option D

Answer: (SHOW ANSWER)

NEW QUESTION: 248

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 eq telnet
!
int Gi0/0
  ipv6 traffic-filter 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 access-map Deny_Telnet in
!
```

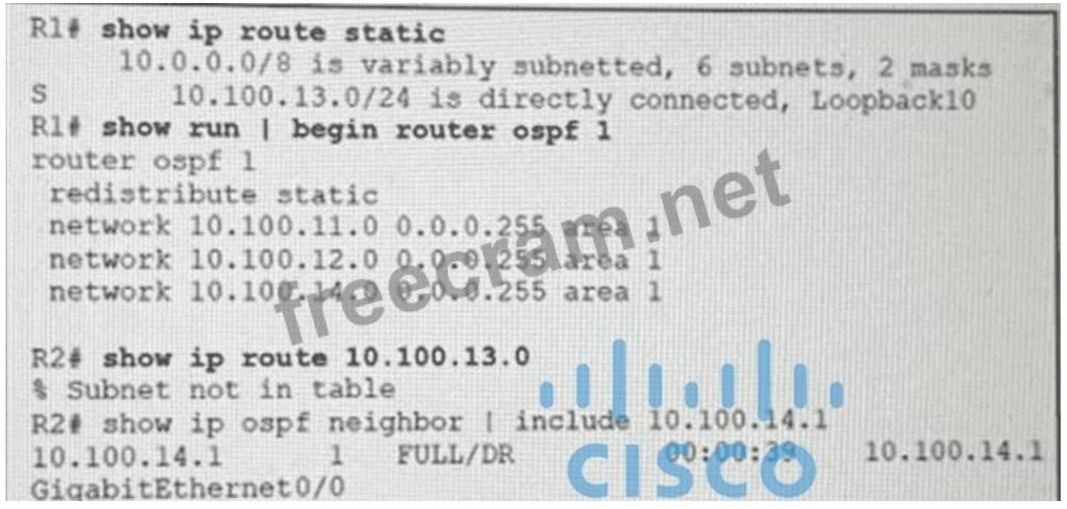
C.
```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
  ipv6 access-map Deny_Telnet in
!
```

D.
```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
  ipv6 traffic-filter Deny_Telnet in
!
```

Answer: (SHOW ANSWER)

NEW QUESTION: 249

:583



Refer to the exhibit. R1 is directly connected to R2 over network 10.100.14.0/24. An engineer configures R1 to advertise a static route that is connected to a local loopback for network 10.100.13.0/24. The network is not in the routing table of R2. Which action resolves the issue?

A. R2 must use a different OSPF process number and should be changed lo ospf 1 to match R1

B. The Loopback interface on R1 is administratively down The interface should be enabled with the no shutdown command

C. The redistribution command isincorrect on R1 The default metric metric 200 should be inducted with the redistribution command.

D. The redistribution command is incorrect on R1 The keyword subnets should be included with the redistribution command

Answer: (SHOW ANSWER)

NEW QUESTION: 250

Refer to the exhibit.

The network administrator configured the Chicago router to mutually redistribute the LA and NewYork 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. Option C
B. Option B
C. Option D
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 251
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 redistributed EIGRP routes as placed into an OSPF area whose area ID matches the EIGRP autonomous system number
D. The administrative distance of the redistributed routes is 170
E. The redistributed EIGRP routes appear as OSPF external type 1
F. The redistributed EIGRP routes appear as OSPF external type 2 routes in the routing table
Answer: (SHOW ANSWER)

NEW QUESTION: 252
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. NHRP mapping is for networks that are local to this router.
B. It was obtained directly from the next-hop server.
C. Data packets are process switches for this mapping entry.
D. The mapping entry was created in response to an NHRP registration request.
E. The NHRP mapping entry cannot be overwritten.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 253

Refer to the exhibit Which action resolves the issue?

A. Configure host IP address in access-list 16

B. Configure SNMP authentication on the router

C. Configure SNMPv3 on the router

D. Configure a valid SNMP community string

Answer: (SHOW ANSWER)

NEW QUESTION: 254

What is an advantage of implementing BFD?

A. BFD provides millisecond failure detection

B. BFD is deployed without the need to run any routing protocol

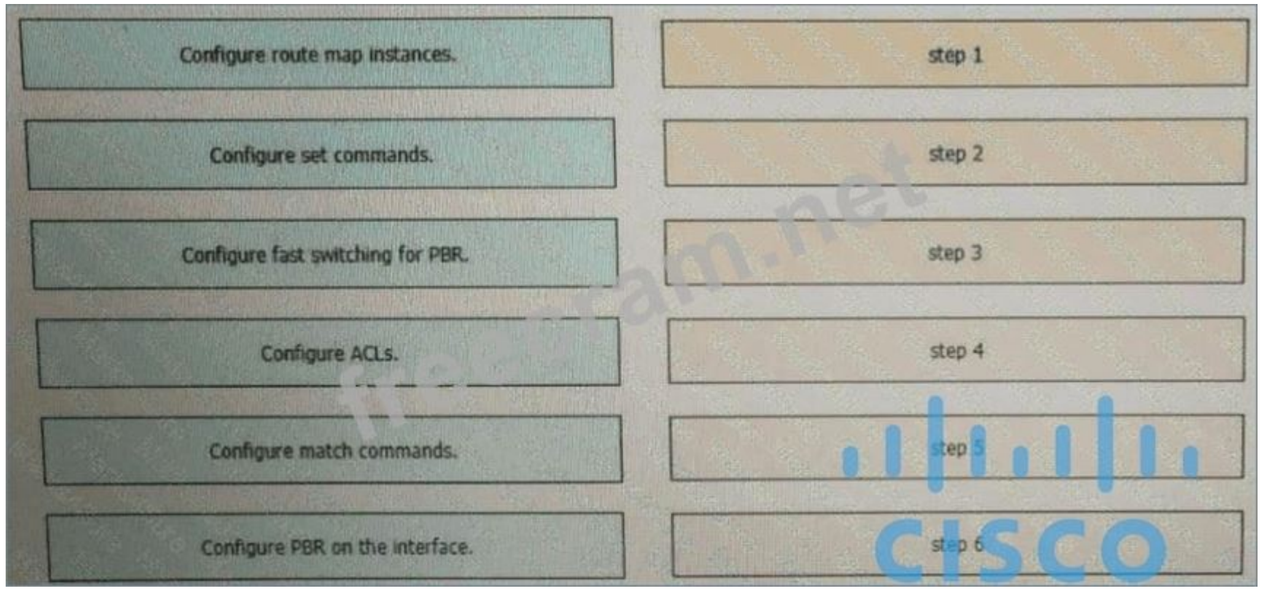
C. BFD provides faster updates for any flapping route.

D. BFD provides better capabilities to maintain the routing table

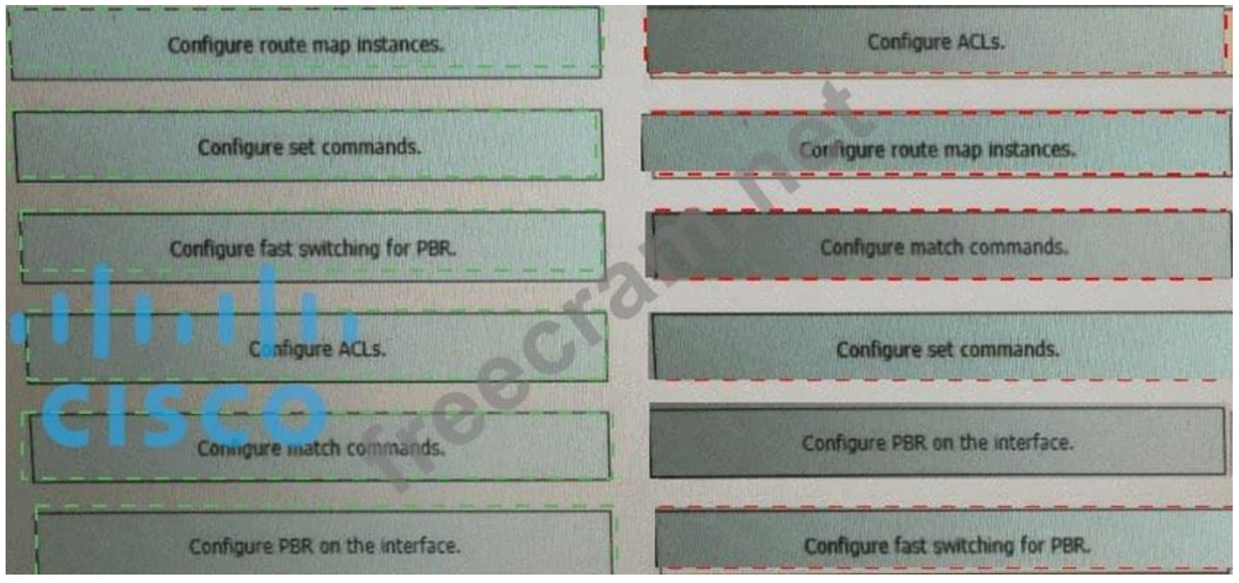
Answer: (SHOW ANSWER)

NEW QUESTION: 255

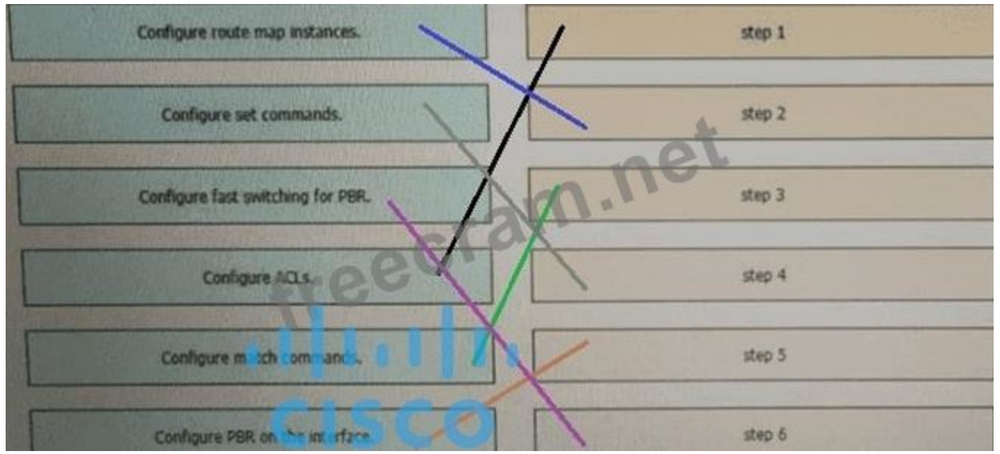
Drag and drop the actions from the left into the correct order on the right to configure a policy to avoid following packet forwarding based on the normal routing path.



Answer:



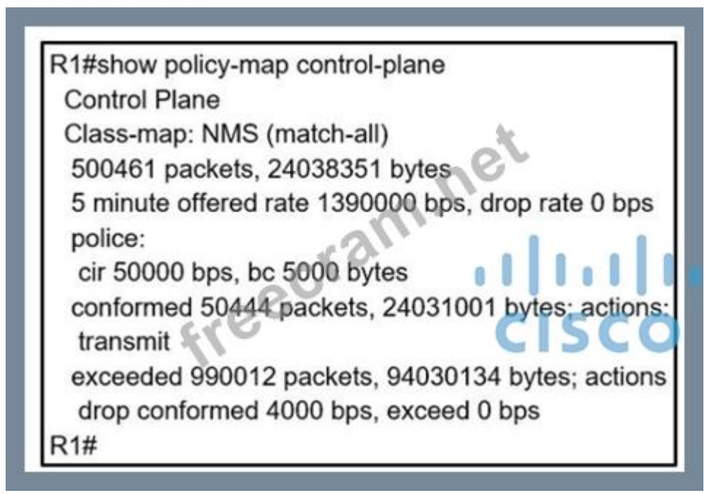
Explanation:



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

NEW QUESTION: 256

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?

A. Remove the exceed-rate command in the class map.

B. Remove the class map NMS from being part of control plane policing.

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: (SHOW ANSWER)

Reference:

https://tools.cisco.com/security/center/resources/copp_best_practices

The class-map NMS in the exhibit did not classify traffic into specific protocols so many packets were dropped. We should create some class-map to classify the receiving traffic. It is also a recommendation of CoPP/CPP policy:

"Developing a CPP policy starts with the classification of the control plane traffic. To that end, the control plane traffic needs to be first identified and separated into different class maps."

NEW QUESTION: 257
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-dient)
       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 nolabel/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 nolabel/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 nolabel/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 nolabel/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 nolabel/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 nolabel/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 nolabel/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 nolabel/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 nolabel/278
```

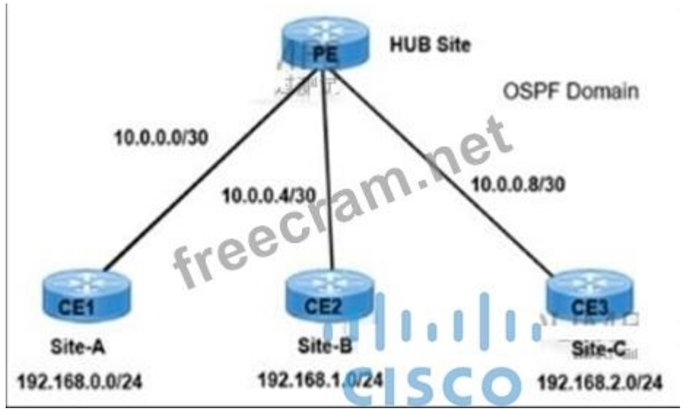
An engineer configured BGP and wants to select the path from 10.77.255.57 as the best path instead of current best path. Which action resolves the issue?

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: (SHOW ANSWER)
From the output, we learn that the current best path is from 10.57.255.11 (which includes "...valid, confed-external, best") and this path is 2 ASes away (64955 65003). Although there are some paths with only 1 AS away (path from 172.16.254.234 for example) but they were not chosen the best path so AS_PATH was not used to determine the best path -> Answers A and answer C are not correct.
All the paths in the output have metric of 0 and this is the lowest (best) value for this attribute. If we configure higher MED then it is less preferred over other paths -> Answer B is not correct.
Only answer D is left but LOCAL_PREF attribute should be configured with higher value to be preferred so we hope "lower LOCAL_PREF" here means higher value. But this is the best answer.

NEW QUESTION: 258
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. Option B
B. Option D
C. Option C
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 259
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. Include the word external in the redistribute command

B. Use a route-map command to redistribute OSPF external routes defined in an access list

C. Include the word internal external in the redistribute command

D. Use a route-map command to redistribute OSPF external routes defined in a prefix list.

Answer: (SHOW ANSWER)

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default. You can use the internal keyword along with the redistribute command under router bgp to redistribute OSPF intra- and inter-area routes.

Use the external keyword along with the redistribute command under router bgp to redistribute OSPF external routes into BGP.

-> In order to redistribute all OSPF routes into BGP, we must use both internal and external keywords. The full command would be (suppose we are using OSPF 1):

redistribute ospf 1 match internal external

Note: The configuration shows match internal external 1 external 2. This is normal because OSPF automatically appends "external 1 external 2" in the configuration. In other words, keyword external = external 1 external 2.

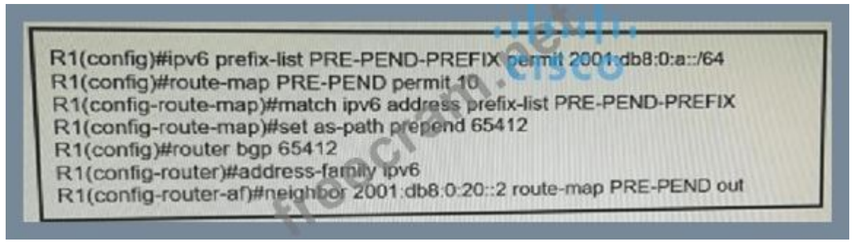
External 1 = O E1 and External 2 = O E2.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redi s.html

NEW QUESTION: 260

Refer to the exhibit.



R1 has a route map configured, which results in a loss of partial IPv6 prefixes for the BGP neighbor, resulting in service degradation. How can the full service be restored?

A. The route map requires a deny 20 statement without set conditions, and this will allow additional prefixes to be advertised.

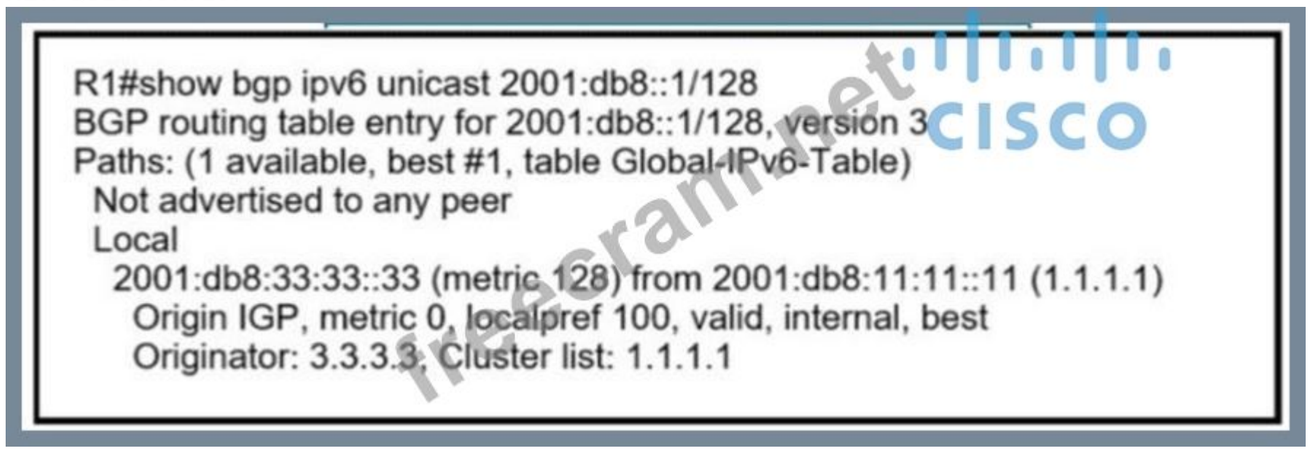
B. The route map requires a permit 20 statement without set conditions, and this will allow additional prefixes to be advertised.

C. The neighbor requires a soft reconfiguration, and this will clear the policy without resetting the BGP TCP connection.

D. The prefix lit requires all prefixes that R1 is advertising to be added to it, and this will allow additional prefixes to be advertised.

Answer: (SHOW ANSWER)

NEW QUESTION: 261



Refer to the exhibit. An engineer examines the BGP update for the IPv6 prefix 2001:db8::1/128. which should have been summarized into a /64 prefix. Which sequence of actions achieves the summarization?

A. R1 is a route reflector client of a RR with a router ID of 1.1.1.1. and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to different ASs. The prefix is not advertised to any peer and must be advertised using the network statement on R3.

B. R1 is a route reflector client of a RR with a router ID of 1.1.1.1. and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to the same AS. Configure an aggregate address on the router with ID 3 3.3.3 for the prefix.

C. R1 is a route reflector with a router ID of 3.3.3.3. and the originator of the prefix is a route reflector client, which has a router ID of 3.3.3.3. Both routers belong to the same AS Configure an aggregate address on the router with ID 1.1.1.1 for the prefix

D. R1 is a route reflector with a router ID of 1.111. and the originator of the prefix is a route reflector client, which has a router ID of 3.3.3.3. Both routers belong to the same AS Configure an aggregate address on the router with ID 1.1.1.1 for the prefix

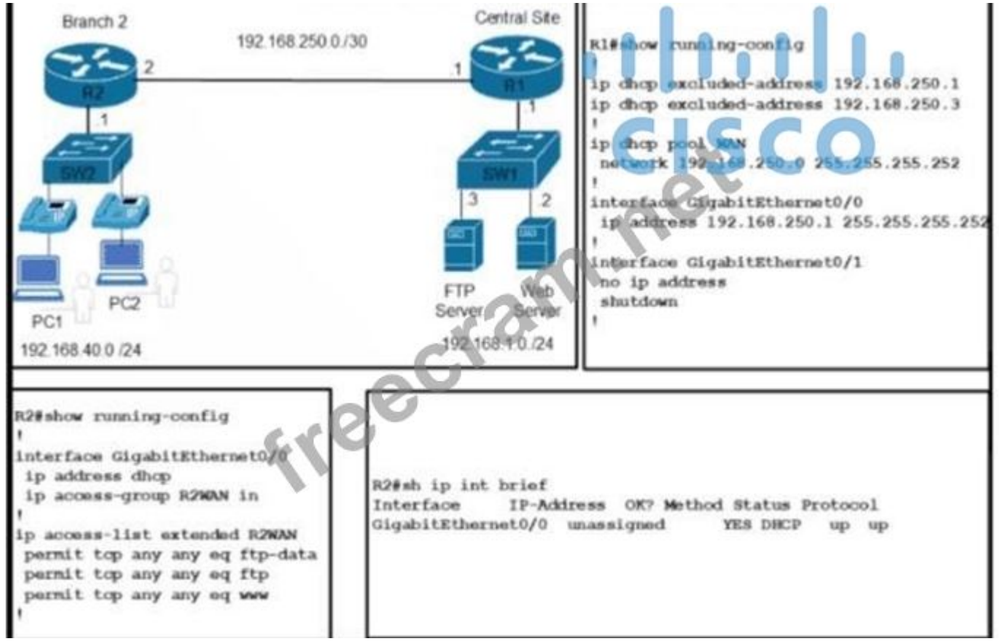
Answer: (SHOW ANSWER)

NEW QUESTION: 262

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?

A. Option D
B. Option B
C. Option A
D. Option C
Answer: (SHOW ANSWER)

NEW QUESTION: 263

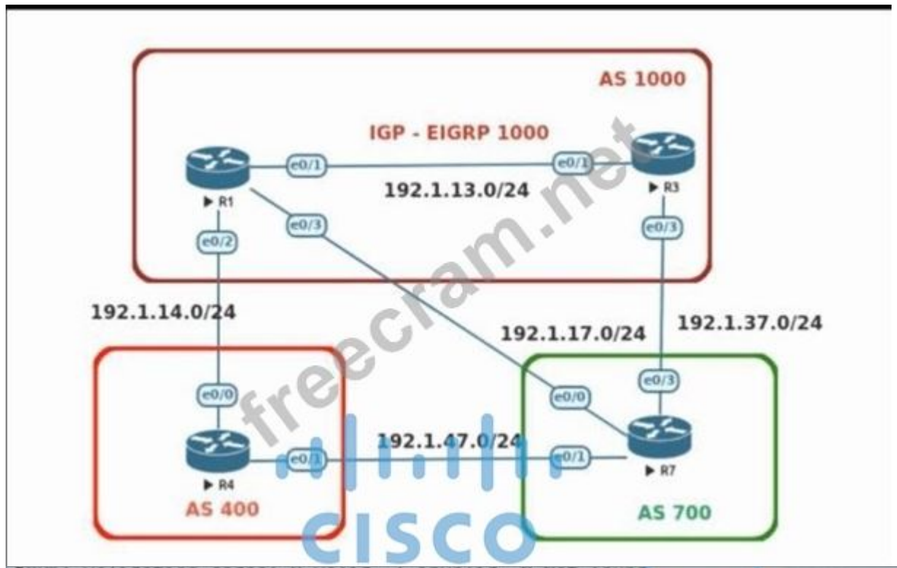


Refer to the exhibit. Which configuration is required for R2 to get the IP address from the DHCP server?

A. interface GigabitEthernet0/0ip access-group R2WAN out
B. ip access-list extended R2WANpermit udp any any eq 67
C. ip access-list extended R2WANpermit udp any any eq 68

D. ip access-list extended R2WANpermit tcp any any eq 68
Answer: C (LEAVE A REPLY)

NEW QUESTION: 264



RPKI validation codes: V valid, I invalid, N Not found

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	1.0.0.0	0.0.0.0	0		32768	i
*>	4.0.0.0	192.1.14.4	0		0	400 i
*>	11.11.11.0/24	0.0.0.0	0		32768	i
*>	44.44.44.0/24	192.1.14.4	0		0	400 i
*>	77.77.77.0/24	192.1.17.7	0		0	700 i
*>	77.77.78.0/24	192.1.17.7	0		0	700 ?
*>	77.77.79.0/24	192.1.17.7	0		0	700 ?
*>	77.77.80.0/24	192.1.17.7	0		0	700 ?

Refer to the exhibit. R1 should have BGP routes marked with an "i" (IGP origin code). Which configuration resolves the issue?

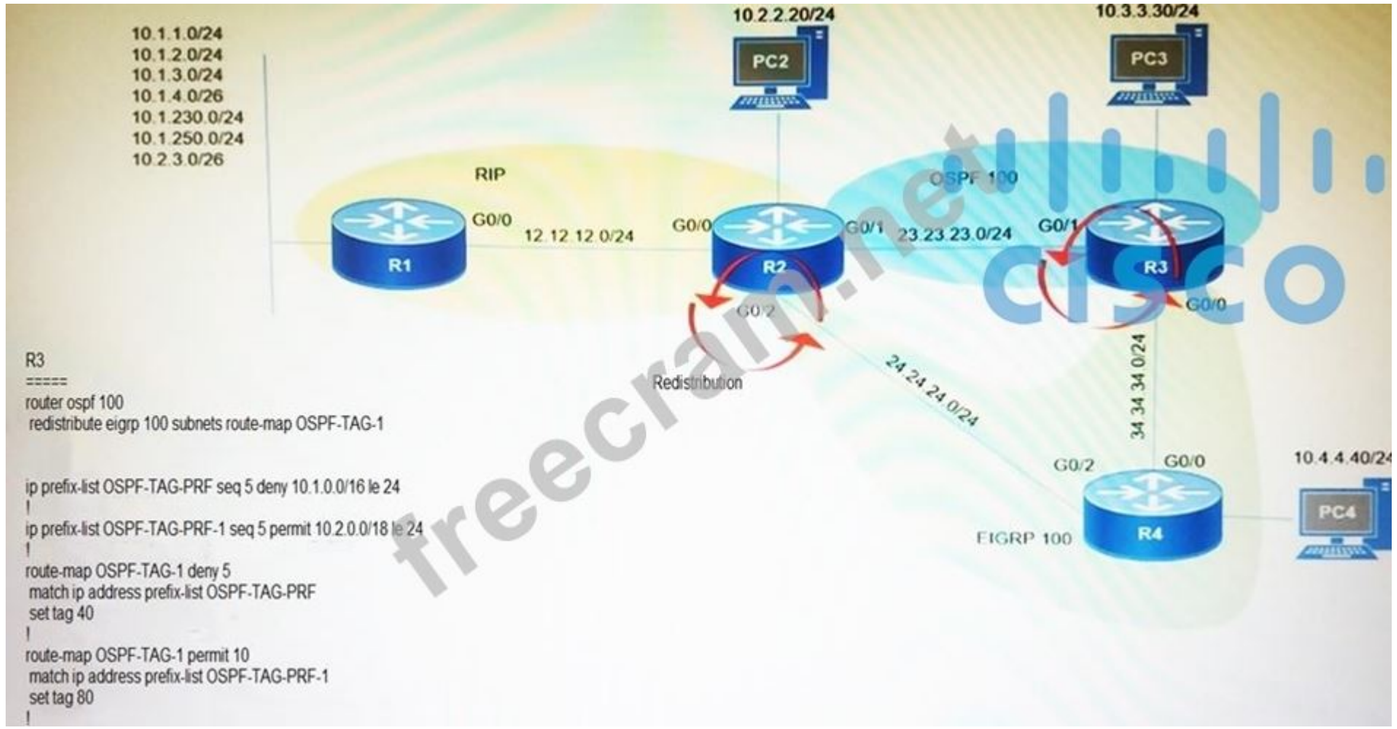
A. R7
route-map RC permit 10
match ip address 1
set metric 1

B. R1
route-map RC permit 10
match ip address 1
set origin igp

C. R1
route-map RC permit 10

match ip address 1
set metric 1
D. R7
route-map RC permit 10
match ip address 1
set origin igp
Answer: (SHOW ANSWER)

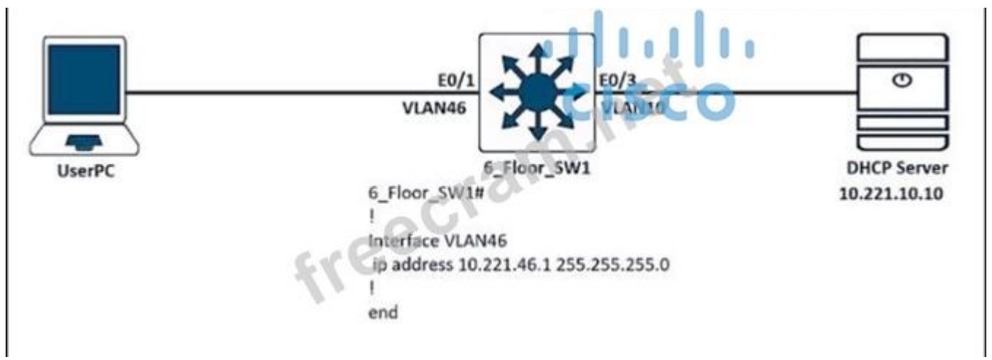
NEW QUESTION: 265
Refer to the exhibit.



Which subnet is redistributed from EIGRP to OSPF routing protocols?
A. 10.1.2.0/24
B. 10.2.2.0/24
C. 10.1.4.0/26
D. 10.2.3.0/26
Answer: (SHOW ANSWER)
NEW QUESTION: 266
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 service provider network to create secure tunnels between customer edge devices

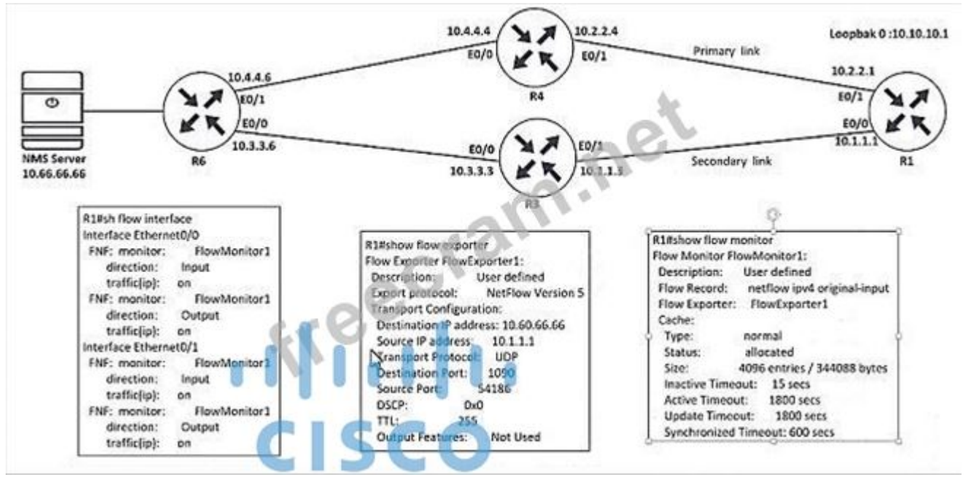
C. set of sites interconnect privately over the Internet for security
D. multiple customer sites interconnect through a service provider network using customer edge to provider edge connectivity
Answer: (SHOW ANSWER)
A Multiprotocol Label Switching(MPLS) Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers.
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/lxvpn/configuration/g uide/b-l3vpn-cg-asr9000-65x/b-l3vpn-cg-asr9000-65x_chapter_010.pdf

NEW QUESTION: 267
Refer to the exhibit.



Users in VLAN46 cannot get the IP from the DHCP server. Assume that all the parameters are configured properly in VLAN 10 and on the DHCP server Which command on interlace VLAN46 allows users to receive IP from the DHCP server?
A. ip dhcp relay information trust-all
B. ip dhcp server 10.221.10.10
C. ip dhcp-addreos 10.221.10.10
D. ip helper-addrets 10.221.10.10
Answer: (SHOW ANSWER)

NEW QUESTION: 268



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. Option B
B. Option C
C. Option D
D. Option A
Answer: (SHOW ANSWER)

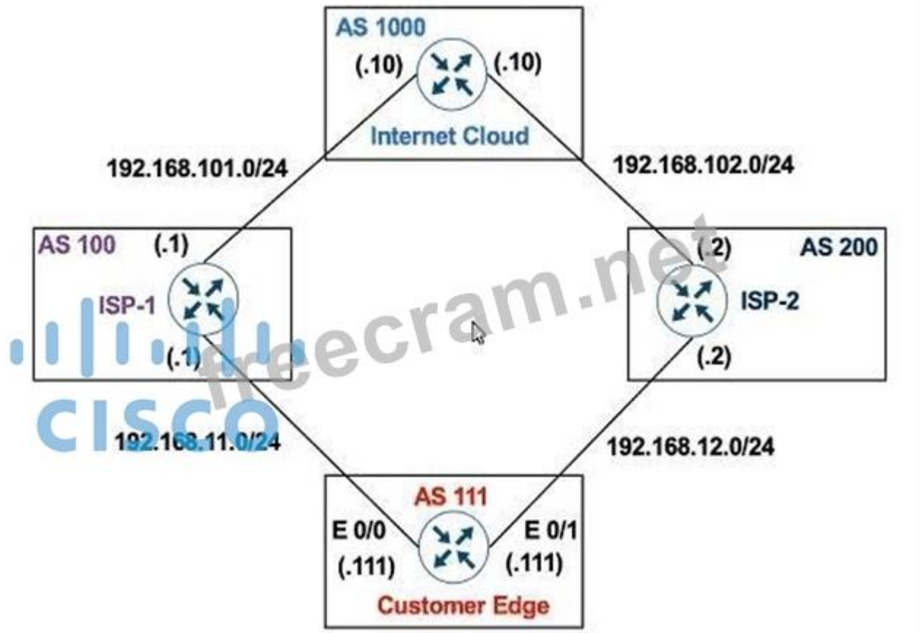
NEW QUESTION: 269

Refer to the exhibit. An engineer is investigating an OSPF issue reported by the Cisco DNA Assurance Center. Which action resolves the issue?

A. An ACL entry blocking multicast on the interfaces Allow multicast through the interface ACL
B. One of the interfaces is using the wrong MTU Match interface MTU on both links

C. One of the interfaces is using the wrong authentication Match interface authentication on both links
D. One of the neighbor links is down Bring the interface up by running shut and no shut
Answer: B (LEAVE A REPLY)

NEW QUESTION: 270




```
ISP-1

ip as-path access-list 1 permit ^111
!
router bop 100
 neighbor 192.168.101.10 remote-as 1000
 neighbor 192.168.11.111 remote-as 111
 neighbor 192.168.11.111 filter-list 1 in
```

Refer to the exhibit. AS 111 mut 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_111_
D. ip as-path access-list 1 permit ^$
Answer: D (LEAVE A REPLY)

NEW QUESTION: 271
Refer to the exhibit.

```
R2#show ip route

Gateway of last resort is not set
   10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
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 (90/4096001 via 10.1.2.2. 00:01:00. FastEthernet0/0
D     10.37.100. 0/24 (90/4096001 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 /110/201 via 10.1.3.2. 00:12:51. FastEthernet0/1
D     10.55.144.0/24 (90/4096001 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 - Passive, 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 10.37.100.0/24, 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. Redistribute the route in EIGRP with metric, delay, and reliability

B. Remove route redistribution in R2 for this route in OSPF

C. Use distribute-list to modify the route as an internal EIGRP route

D. Use distribute-list to filter the external router in OSPF

Answer: (SHOW ANSWER)

NEW QUESTION: 272

Refer to the exhibit.

```
R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf1
R1(config-router)#redistribute rip subnets route-map ADD
```

Which statement about R1 is true?

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. RIP routes are redistributed to OSPF without any changes.

D. R1 adds one to the metric for RIP learned routes before redistributing to OSPF.

Answer: (SHOW ANSWER)

NEW QUESTION: 273

Refer to the exhibit.

```
R1#show ip route ospf

     10.0.0.0/24 is subnetted, 7 subnets

O E2    10.4.9.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0

                 [110/200] via 10.4.15.5, 00:06:43,
FastEthernet0/1

O IA    10.4.27.0 [110/2] via 10.4.15.5, 00:06:44,
FastEthernet0/1

O E2    10.4.49.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0
```

An engineer configures two ASBRs 10 4 17.6 and 10 4 15 5 in an OSPF network to redistribute routes from EIGRP However, both ASBRs show the EIGRP routes as equal costs even though the next-hop router 10 4 17 6 is closer to R1 How should the network traffic to the EIGRP prefixes be sent via 10 4.17.6?

A. The administrative distance should be raised to 120 from the ASBR 104 17 6

B. The ASBR 10 4 17 6 should assign a tag to match and assign a lower metnc on R1

C. The redistributed prefixes should be advertised as Type 1

D. The administrative distance should be raised to 120 from the ASBR 104.17.6

E. The administrative distance should be raised to 120 from the ASBR 10.4.15 5.

F. The admitstrative distance should be raised to 120 from the ASBR 104 15.5.

G. The ASBR 10 4 17 6 should assign a tag to match and assign a tower metnc on R1

H. The redistributed prefixes should be advertised as Type 1.

Answer: (SHOW ANSWER)

NEW QUESTION: 274

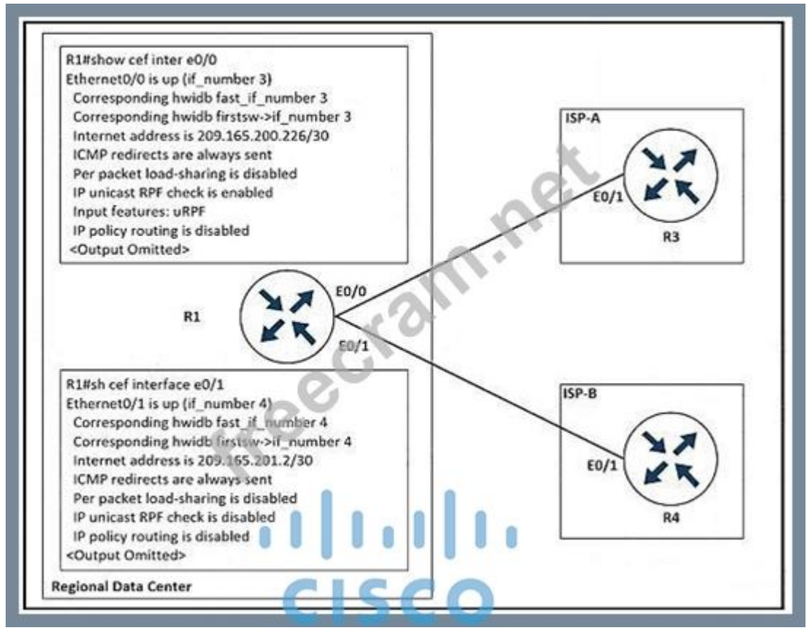
How does LDP operate in an MPLS network?

A. LDP notification messages allow LERs to exchange label information to determine the next hops within a particular LSP.

B. When topology changes occur such as a router failure, LDP generates peer discovery messages that terminate the LDP season to propagate an LSP change.

C. Peer routers establish the LDP session, and the LDP neighbors maintain and terminate the session by exchanging messages
D. When an adjacent LSR receives LDP discovery messages. TCP two-way handshake ensures that the LDP session has unidirectional connectivity.
Answer: (SHOW ANSWER)

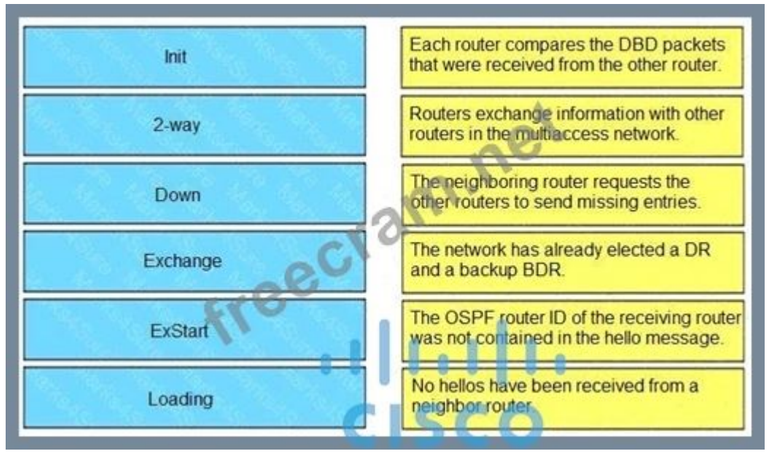
NEW QUESTION: 275



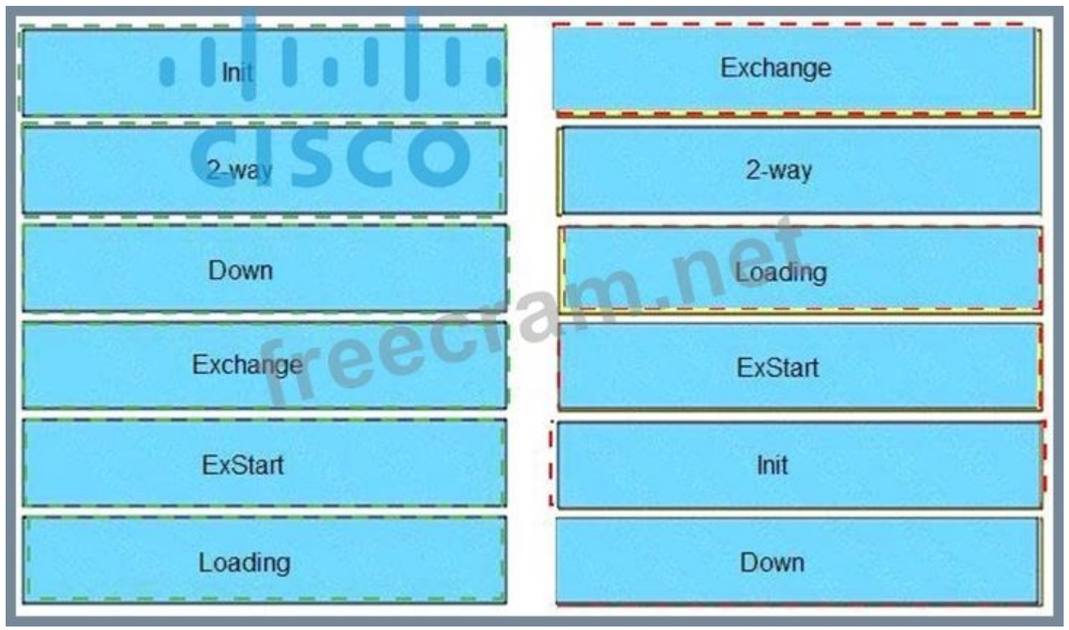
Refer to the exhibit. The company implemented uRPF to address an antispoofing attack. A network engineer received a call from the IT security department that the regional data center is under an IP attack Which configuration must be implemented on R1 to resolve this issue?

A. Option B
B. Option A
C. Option C
D. Option D
Answer: (SHOW ANSWER)

NEW QUESTION: 276
Drag and drop the OSPF adjacency states from the left onto the correct descriptions on the right.



Answer:



Explanation:

Table Description automatically generated
(Reference: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml) Reference: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html Down This is the first OSPF neighbor state. It means that no information (hellos) has been received from this neighbor, but hello packets can still be sent to the neighbor in this state.
During the fully adjacent neighbor state, if a router doesn't receive hello packet from a neighbor within the Router Dead Interval time (RouterDeadInterval = 4*HelloInterval by default) or if themanually configured neighbor is being removed from the configuration, then the neighbor state changes from Full to Down.
Attempt
This state is only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.
Init
This state specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the sender's router ID in its hello packet as an acknowledgment that it received a valid hello packet.
2-Way
This state designates that bi-directional communication has been established between two routers. Bi- directional means that each router has seen the other's hello packet. This state is attained when the router receiving the hello packet sees its own Router ID within the received hello packet's neighbor field. At this state, a router decides whether to become adjacent with this neighbor. On broadcast media and non-broadcast multiaccess networks, a router becomes full only with the designated router (DR) and the backup designated router (BDR); it stays in the 2-way state with all other neighbors. On Point-to-point and Point-to-multipoint networks, a router becomes full with all connected routers.
At the end of this stage, the DR and BDR for broadcast and non-broadcast multiaccess networks are elected.
For more information on the DR election process, refer to DR Election.
Note: Receiving a Database Descriptor (DBD) packet from a neighbor in the init state will also a cause a transition to 2-way state.
Exstart
Once the DR and BDR are elected, the actual process of exchanging link state information can start between the routers and their DR and BDR. (ie. Shared or NBMA networks).
In this state, the routers and their DR and BDR establish a master-slave relationship and choose the initial sequence number for adjacency formation. The router with the higher router ID becomes the master and starts the exchange, and as such, is the only router that can increment the sequence number. Note that one would logically conclude that the DR/BDR with the highest router ID will become the master during this process of master-slave relation. Remember that the DR/BDR election might be purely by virtue of a higher priority configured on the router instead of highest router ID. Thus, it is possible that a DR plays the role of slave.
And also note that master/slave election is on a per-neighbor basis.
Exchange
In the exchange state, OSPF routers exchange database descriptor (DBD) packets. Database descriptors contain link-state advertisement (LSA) headers only and describe the contents of the entire link-state database. Each DBD

packet has a sequence number which can be incremented only by master which is explicitly acknowledged by slave. Routers also send link-state requestpackets and link-state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the routers link-state database to check if new or more current link-state information is available with the neighbor.
Loading
In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, routers send link-state request packets. The neighbor then provides the requested link-state information in link-state update packets. During the adjacency, if a router receives an outdated or missing LSA, it requests that LSA by sending a link-state request packet. All link-state update packets are acknowledged.
Full
In this state, routers are fully adjacent with each other. All the router and network LSAs are exchanged and the routers' databases are fully synchronized.
Full is the normal state for an OSPF router. If a router is stuck in another state, it is an indication that there are problems in forming adjacencies. The only exception to this is the 2-way state, which is normal in a broadcast network. Routers achieve the FULL state with their DR and BDR in NBMA/broadcast media and FULL state with every neighbor in the remaining media such as point-to-point and point-to-multipoint.
Note: The DR and BDR that achieve FULL state with every router on the segment will display FULL
/DROTHER when you enter the show ip ospf neighbor command on either a DR or BDR. This simply means that the neighbor is not a DR or BDR, but since the router on which the command was entered is either a DR or BDR, this shows the neighbor as FULL/DROTHER.
Reference: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html Reference: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml) Reference: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

NEW QUESTION: 277
Refer to the exhibit.

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.10.1            Se1/0            12 00:00:39    1   5000  2  0
*Jan  1 15:40:21.295: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is down: retry limit exceeded
*Jan  1 15:40:51.567: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is up: new adjacency
*Jan  1 15:42:11.107: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is down: retry limit exceeded
*Jan  1 15:42:14.879: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is up: new adjacency


R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
```

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-chain name on both routers

B. Configure a matching key-id number on both routers

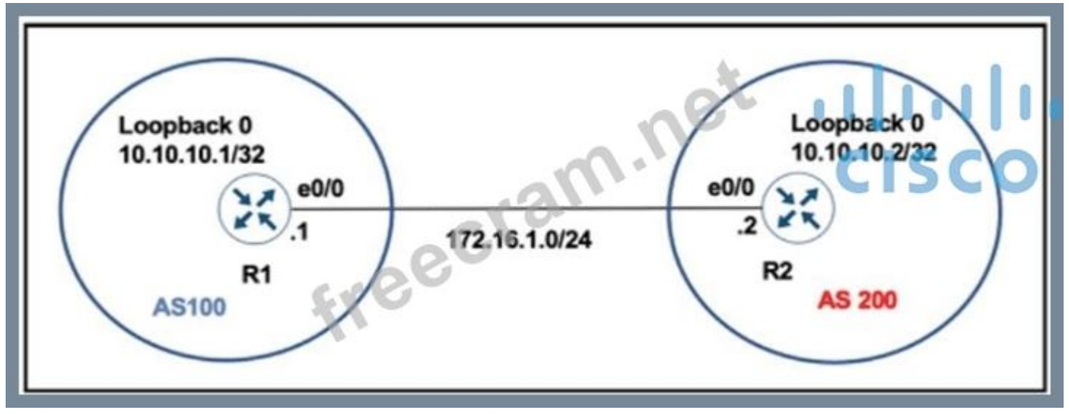
C. Configure a matching authentication type on both router

D. Configure a matching lowest key-id on both routers

Answer: (SHOW ANSWER)

NEW QUESTION: 278

:576



Refer to the exhibit. R1 and R2 have been configured where the neighbor relationship must be authenticatedusmgMD5:

```
R1
router bgp 100
 neighbor 172.16.1.2 remote-as 200
 neighbor 172.16.1.1 password cisco123


R2
router bgp 200
 neighbor 172.16.1.1 remote-as 100
 neighbor 172.16.1.1 password cisco
```

The neighbor relationship is not coming up. Which configuration resolves the issue?

R1

```
router bgp 100
 neighbor 172.16.1.2 password cisco
```

R2

```
router bgp 200
 neighbor 172.16.1.1 password cisco123
```

R1

```
router bgp 100
 neighbor 172.16.1.2 password MD5 cisco123
```

R2

```
router bgp 200
 neighbor 172.16.1.1 password MD5 cisco123
```

R1

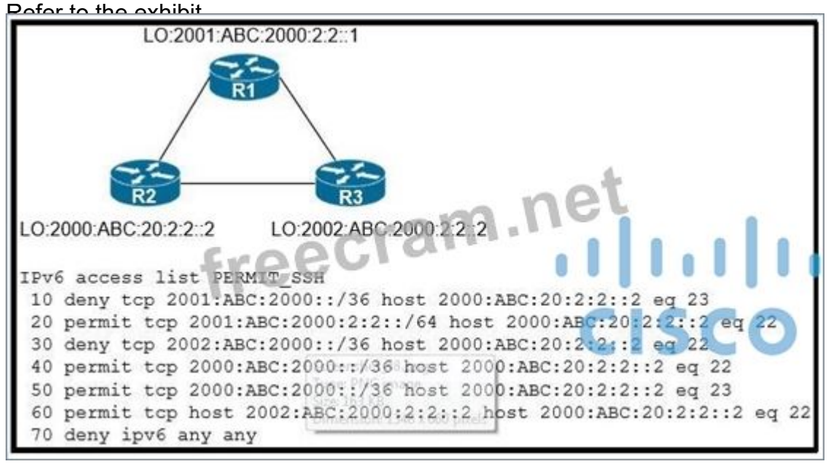
```
router bgp 100
 neighbor 172.16.1.2 password MD5 cisco
```

R2

```
router bgp 100
 neighbor 172.16.1.1 password MD5 cisco
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: B (LEAVE A REPLY)

NEW QUESTION: 279
Refer to the exhibit



An IPv6 network was newly deployed in the environment and the help desk reports that R3 cannot SSH to the R2s Loopback interface. Which action resolves the issue?

A. Remove line 60 from the access list.

B. Modify line 10 of the access list to permit instead of deny.

C. Remove line 70 from the access list.

D. Modify line 30 of the access list to permit instead of deny.

Answer: (SHOW ANSWER)