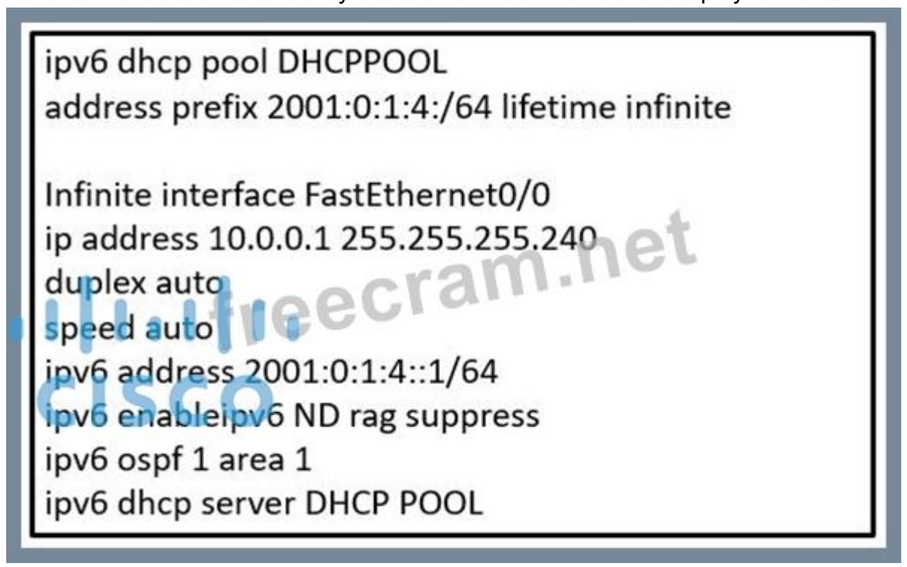
# Cisco.300-410.v2026-06-08.q377

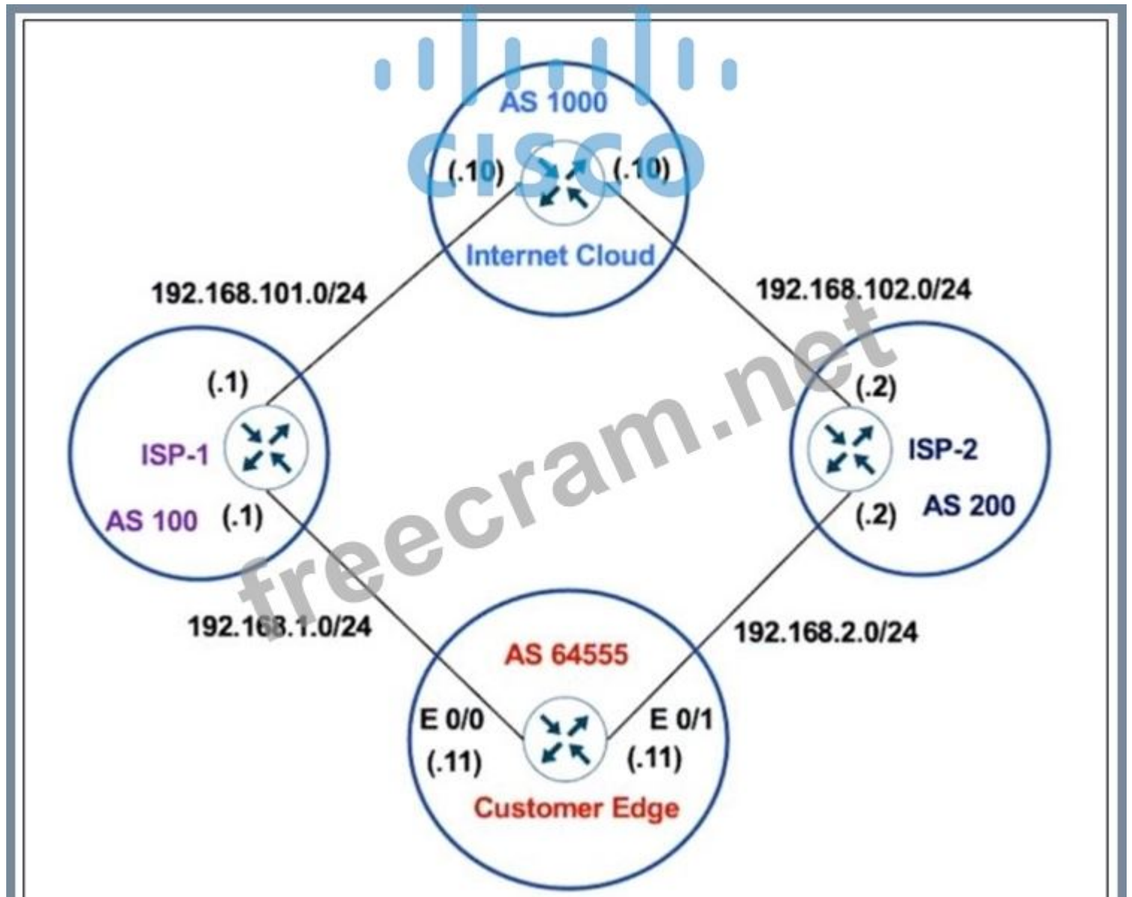
| | |
|---|---|
| **Exam Code:** | 300-410 |
| **Exam Name:** | Implementing Cisco Enterprise Advanced Routing and Services |
| **Certification Provider:** | Cisco |
| **Free Question Number:** | 377 |
| **Version:** | v2026-06-08 |
| **# of views:** | 111 |
| **# of Questions views:** | 4130 |
| https://www.freecram.net/torrent/Cisco.300-410.v2026-06-08.q377.html | |

**NEW QUESTION: 1**
Refer to the exhibit. Reachability between servers in a network deployed with DHCPv6 is unstable. Which command must be removed from the configuration to make DHCPv6 function?




**A.** ipv6 dhcp server DHCPPOOL
**B.** ipv6 address 2001:0:1:4::/64
**C.** ipv6 nd ra suppress
**D.** address prefix 2001:0:1:4::/64 lifetime infinite infinite
**Answer: (SHOW ANSWER)**
In IPv6, hosts locate a router through Router Advertisement (RA) messages sent from routers instead of by DHCP; IPv6-enabled routers that support dynamic address assignment are expected to announce themselves on the network to all clients. As such, DHCPv6 does not include any gateway information.

**NEW QUESTION: 2**
Refer to the 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 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
```

**B.**
```
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
```

**C.**
```
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
```

**D.**
```
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
```

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 3**

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
```

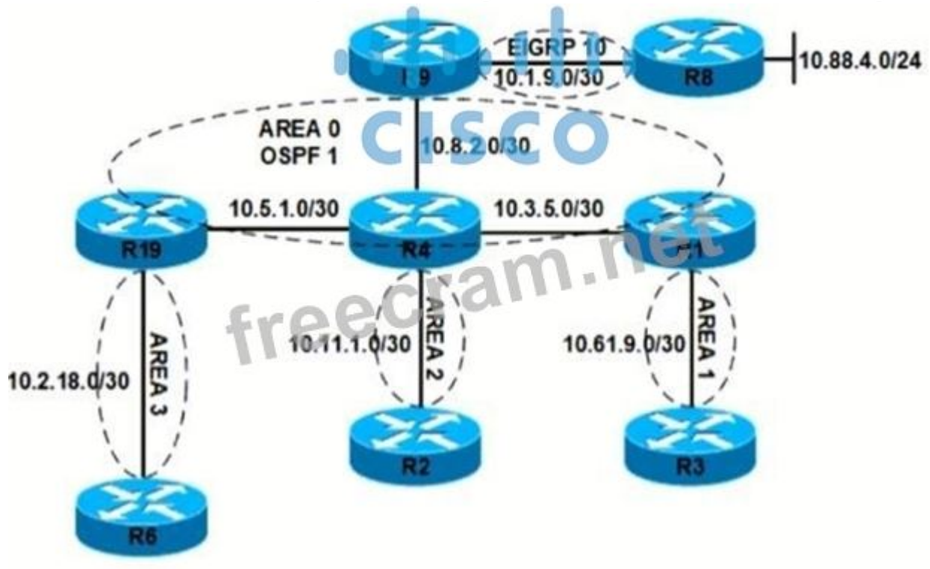
The network administrator is not getting the desired result for the SNMP traffic and SNMP traffic is getting dropped frequently. Which set of configurations resolves the issue?

**A.**
```
policy-map PM-COPP
class CM-SNMP
no police 1000 conform-action transmit
police 1000000 conform-action transmit
```

**B.**
```
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
**C.** no access-list 100
access-list 100 permit tcp host 192.168.1.11 any eq 161
**D.** 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
!
control-plane
no service-policy input PM-COPP
!
interface E 0/0
service-policy input PM-COPP
!
interface E 0/1
service-policy input PM-COPP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 4**
Refer to the exhibit. An engineer recently modified the configuration for area 3 to accept only type
1, 2, and 3 LSAs. Immediately after the changes, users connected to router R6 began to report connectivity issues. Which configuration restores connectivity to R6 and meets the requirement?



A.
```
(19#
router ospf 1
  area 3 nssa
  network 10.2.18.0 0.0.0.3 area 3
  network 10.5.1.0 0.0.0.3 area 0

(6#
router ospf 1
  area 3 nssa
  network 10.2.18.0 0.0.0.3 area 3
  network 10.6.6.255 0.0.0.0 area 1
```

B.
```
R19#
router ospf 1
  area 3 stub
  network 10.2.18.0 0.0.0.3 area 3
  network 10.5.1.0 0.0.0.3 area 0

R6#
router ospf 1
  network 10.2.18.0 0.0.0.3 area 3
  network 10.6.6.255 0.0.0.0 area 3
```

C.
```
R19#
router ospf 1
  area 3 stub
  network 10.2.18.0 0.0.0.3 area 3
  network 10.5.1.0 0.0.0.3 area 0

R6#
router ospf 1
  router-id 10.6.6.255
  area 3 stub
  network 10.2.18.0 0.0.0.3 area 3
  network 10.6.6.255 0.0.0.0 area 3
```

D.
```
R19#
router ospf 1
  area 3 stub no-summary
  network 10.2.18.0 0.0.0.3 area 3
  network 10.5.1.0 0.0.0.3 area 0

R6#
router ospf 1
  network 10.2.18.0 0.0.0.3 area 3
  network 10.6.6.255 0.0.0.0 area 3
```

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 5**

Refer to the exhibit. The default route is not advertised to the neighboring router. Which action resolves the issue?

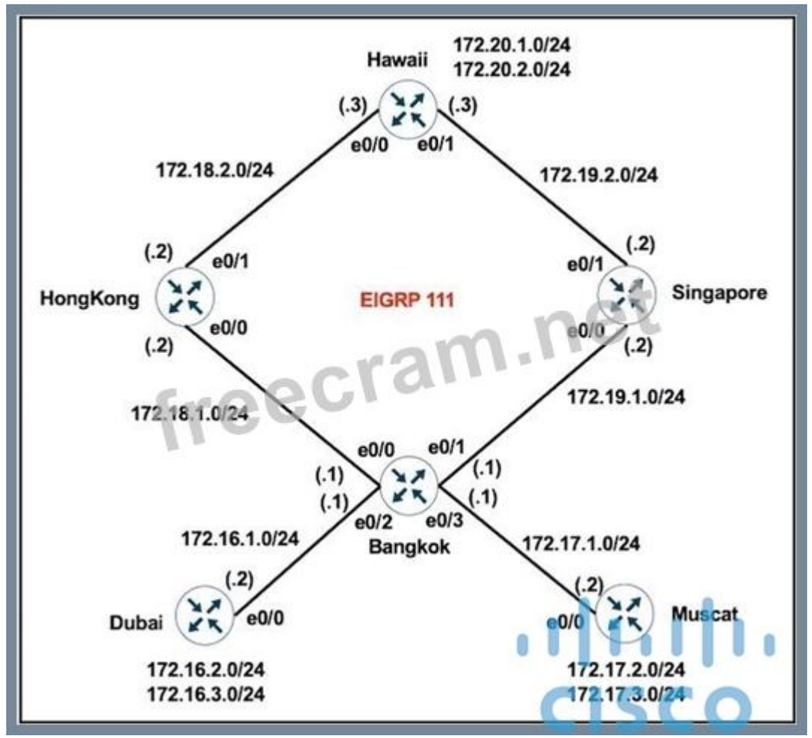
```
CPE# show ip route static
<output omitted>
S*    0.0.0.0/0 is directly connected, Dialer0
S     198.51.100.0/24 [1/0] via 192.168.1.1
S     203.0.113.0/24 [1/0] via 192.168.2.1

CPE# show run | section router ospf
router ospf 1
 redistribute static subnets

CPE# show ip ospf database | begin Type-5
       Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
198.51.100.0    192.168.0.1     14          0x80000001 0x0007D0 0
203.0.113.0     192.168.0.1     14          0x80000001 0x009C5C 0
```



**A.** Configure the default-information originate command under OSPF
**B.** Configure OSPF on the Dialer0 interface.
**C.** Configure the redistribute static metric 200 subnets command under OSPF.
**D.** Configure the network 0.0.0.0 255.255.255.255 area 0 command under OSPF
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 6**
What happens when two EIGRP peers have mismatched K values?
**A.** The two devices are unable to correctly perform unequal-cast load balancing
**B.** The two devices fail to perform EIGRP graceful shutdown when one device goes down
**C.** The two devices fail to from an adjacency
**D.** The two devices are unable to correctly perform equal-cost routing
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 7**
Refer to the exhibit. Bangkok is using ECMP to reach the 172.20.2.0/24 network. The network administrator must configure it in such a way that traffic from 172.16.2.0/24 network uses the Singapore router as the preferred route. Which set of configurations accomplishes this task?






**A.** Dubai

```
access-list 101 permit ip 172.16.2.0 0.0.0.255 172.20.2.0 0.0.0.255
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.19.1.2
!
interface Ethernet0/0
ip policy route-map PBR1
```

**B.** Bangkok

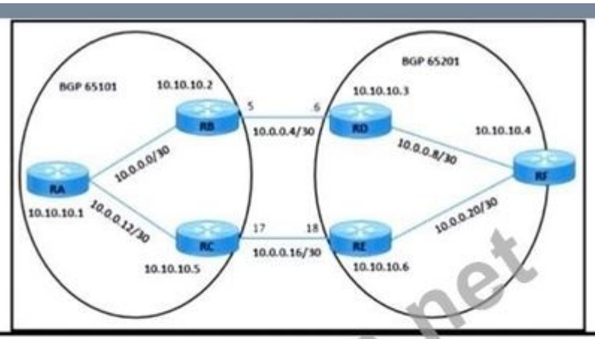
```
access-list 101 permit ip 172.16.2.0 0.0.0.255 172.20.2.0 0.0.0.255
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.19.1.2
!
interface Ethernet0/1
ip policy route-map PBR1
```

**C.** Dubai

```
access-list 101 permit ip 172.16.2.0 0.0.0.255 172.20.2.0 0.0.0.255
```

!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.19.1.2
set ip next-hop peer-address
!
interface Ethernet0/0
ip policy route-map PBR1
**D.** Bangkok
access-list 101 permit ip 172.16.2.0 0.0.0.255 172.20.2.0 0.0.0.255
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.19.1.2
!
interface Ethernet0/2
ip policy route-map PBR1
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 8**
Refer to the exhibit. A NOC team receives a ticket that data traffic from RA to RF is not forwarded when the link between the RC-RE path goes down. Alll routers leam loopback IP through the IGP protocol. Which configuration resolves the issue?




```
RB#
*Sep 19 00:53:43.002: BGPNSF state: 10.10.10.3 went from nsf_not_active to
nsf_not_active
*Sep 19 00:53:43.006: BGP: 10.10.10.3 went from Established to Idle
*Sep 19 00:53:43.006: %BGP-5-ADJCHANGE: neighbor 10.10.10.3 Down User reset
*Sep 19 00:53:43.006: BGP: 10.10.10.3 closing
*Sep 19 00:53:43.106: BGP Router: unhandled major event code 128, minor 0

RD#show  ip bgp neighbors 10.10.10.2
BGP neighbor is 10.10.10.2,  remote AS 65101, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:01:35, last write 00:01:35, hold time is 180, keepalive
interval is 60 seconds
Default minimum time between advertisement runs is 30 seconds
 Address tracking is enabled, the RIB does have a route to 10.10.10.2
  Connections established 11; dropped 11
  Last reset 00:01:36, due to Peer closed the session
  External BGP neighbor may be up to 3 hops away.
  Transport(tcp) path-mtu-discovery is enabled
  No active TCP connection
```

**A.** RD(config)#router bgp 65201
RD(config-router)# neighbor 10.10.10.2 update-source loopback 0
**B.** RD(config-router)# neighbor bgp 65101
RD(config-router)# neighbor 10.10.10.3 ebgp-multihop 3
**C.** RB(config)# router bgp 65101
RD(config-router)# neighbor 10.10.10.3 update-source loopback 0
**D.** RD(config)# router bgp 65201
RD(config-router)# neighbor 10.10.10.2 ebgp-multihop 3
**Answer: (SHOW ANSWER)**
The issue arises because eBGP sessions between RD and RB fail when the direct link goes down. By default, eBGP sessions require a single hop between neighbors. However, in this topology, when the RC-RE path goes down, the traffic must traverse multiple hops (via the loopback addresses).
To resolve the issue, enable eBGP multihop: The ebgp-multihop command allows the BGP session to establish across multiple hops. In this case, ebgp-multihop 3 is configured on RD to ensure the session with RB is maintained. Ensure that loopback addresses are used as the BGP neighbor source and are reachable through IGP.
This configuration allows BGP to maintain the session even when the direct link fails, ensuring traffic can still flow through the alternate path.

**NEW QUESTION: 9**
What is the function of penultimate hop popping?
**A.** The last P router in the path pops off the transport label before traffic is forwarded toward the PE.

**B.** The second to last P router in the path pops off the VPN label before traffic is forwarded to the last P router.
**C.** The transport label is popped off at the egress LSR, and unlabeled traffic is forwarded toward the CE.
**D.** The VPN label is popped off at the egress LSR, and unlabeled traffic is forwarded toward the CE.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 10**
Refer to the exhibit. Which control plan policy limits BGP traffic that is destined to the CPU to 1 Mbps and ignores BGP traffic that is higher rate?

```
Cat3850-Stack-2# show policy-map

Policy Map LIMIT_BGP
  Class BGP
    drop

Policy Map SHAPE_BGP
  Class BGP
    Average Rate Traffic Shaping
    cir 10000000 (bps)

Policy Map POLICE_BGP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action transmit

Policy Map COPP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action drop
```

**A.** policy-map SHAPE_BGP
**B.** policy-map LIMIT_BGP
**C.** policy-map POLICE_BGP
**D.** policy-map COPP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 11**
How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?
**A.** by RD

**B.** by address family
**C.** by MP-BGP
**D.** byRT
**Answer: (SHOW ANSWER)**
The route-distinguisher argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter a route distinguisher (RD) in either of these formats:
- 16-bit AS number: your 32-bit number, for example, 101:3
- 32-bit IP address: your 16-bit number, for example, 10.0.0.1:1

**NEW QUESTION: 12**
Refer to the exhibit. An engineer is trying to generate a summary route in OSPF for network
10.0.0.0/8, but the summary route does not show up in the routing table. Why is the summary route missing?

```
Router#show ip route
<output omitted>
Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
O        192.168.1.1 [110/11] via 192.168.12.1, 16:56:40, Ethernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback0
L        192.168.2.2/32 is directly connected, Loopback0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Ethernet0/1
L        192.168.3.1/32 is directly connected, Ethernet0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.2/32 is directly connected, Ethernet0/0
Router#show running-config | section ospf
router ospf 1
 summary-address 10.0.0.0 255.0.0.0
 redistribute static subnets
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
Router#
```

**A.** The summary route is not visible on this router, but it is visible on other OSPF routers in the same area.
**B.** The summary-address command is used only for summary prefixes between areas.
**C.** The summary route is visible only in the OSPF database not in the routing table.
**D.** There is no route for a subnet inside 10.0.0.0/8, so the summary route is not generated.
**Answer: (SHOW ANSWER)**

The "summary-address" is only used to create aggregate addresses for OSPF at an autonomous system boundary. It means this command should only be used on the ASBR when you are trying to summarize externally redistributed routes from another protocol domain or you have a NSSA area. But a requirement to create a summarized route is:
"The ASBR compares the summary route's range of addresses with all routes redistributed into OSPF on that ASBR to find any subordinate subnets (subnets that sit inside the summary route range). If at least one subordinate subnet exists, the ASBR advertises the summary route." But in this case we found no prefix that belongs to 10.0.0.0/8. Therefore a summarized route for this subnet could not be created.
Note:
+ If a prefix of this subnet exists in the routing table then after the summarization is performed, we will see such an entry:
Router# show ip route
- output omitted -
0 10.0.0.0/8 is a summary via null0

**NEW QUESTION: 13**
Refer to the exhibit. An engineer is trying to log in to R1 via R3 loopback address. Which action resolves the issue?


**A.** Remove the IPv6 traffic filter from R1, which is blocking the Telnet.
**B.** Add transport input none
**C.** Add transport input SCP
**D.** Remove the IPv6 traffic from R1, which is blocking the SSH
**Answer: A (LEAVE A REPLY)**

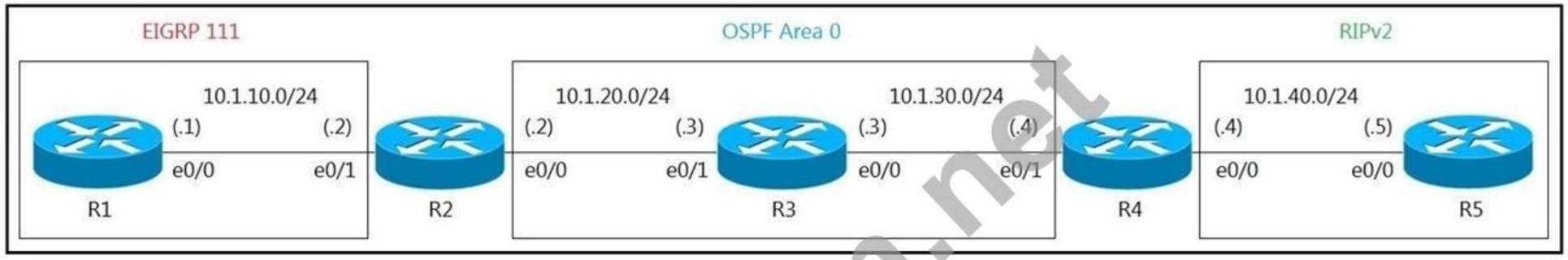
**NEW QUESTION: 14**

Refer to the exhibit. Network operations cannot read or write an configuration on the device with this configuration from the operation subnet. Which two configuration fix the issue? (Choose two.)

```
snmp-server community ciscotest 1
snmp-server host 192.168.1.128 ciscotest
snmp-server enable traps bgp
```

**A.** Configure SNMP rw permission in addition to community ciscotest.
**B.** Modify access list 1 and allow operations subnet in the access list.
**C.** Modify SNMP rw permission in addition to version 1.
**D.** Configure SNMP rw permission in addition to version 1.
**E.** Configure SNMP rw permission in addition to community ciscotest 1.
**Answer: (SHOW ANSWER)**
Configure SNMP rw permission: Changes the community from the default read-only to read-write, allowing configuration changes.
Modify access list 1: Ensures the operation subnet has the underlying network permission to reach the SNMP service.

**NEW QUESTION: 15**
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?




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

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

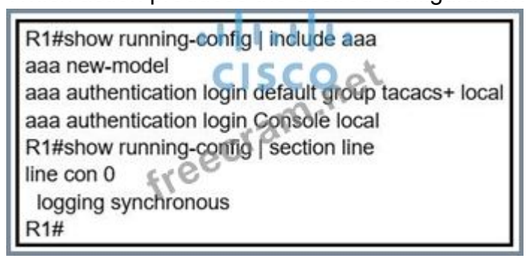
**A.** R2
route-map E20 deny 20
R4
route-map O2R deny 10
match tag 111
!
router rip
redistribute ospf 1 route-map O2R metric 1

**B.** R4
route-map O2R deny 10
match tag 111
!
router rip
redistribute ospf 1 route-map O2R metric 1

**C.** R4
route-map O2R deny 10
match tag 111
route-map O2R permit 20
!
router rip
redistribute ospf 1 route-map O2R metric 1
**D.** R4
route-map O2R permit 10
match tag 111
route-map O2R deny 20
!
router rip
redistribute ospf 1 route-map O2R metric 1
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 16**
An engineer is implementing a coordinated change with a server team. As part of the change, the engineer must configure interlace GigabitEthernet2 in an existing VRF "RED" then move the interface to an existing VRF "BLUE" when the server team is ready.
The engineer configured interface GigabitEthemet2 in VRF "RED".
interface GigabitEthernet2
description Migration ID: B410A82D0935G35
vrf forwarding RED
ip address 10.0.0.0 255.255.255.254
negotiation auto
Which configuration completes the change?
**A.** interface GigabitEthernet2
no ip address
ip address 10.0.0.0 255.255.255.254
vrf forwarding BLUE
**B.** interface GigabitEthernet2
no vrf forwarding RED
vrf forwarding BLUE
ip address 10.0.0.0 255.255.255.254
**C.** interface GigabitEthernet2
no ip address
vrf forwarding BLUE
**D.** interface GigabitEthernet2
no vrf forwarding RED
vrf forwarding BLUE
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 17**
Refer to the exhibit. An engineer is trying to configure local authentication on the console line, but the device is trying to authenticate using TACACS+.
Which action produces the desired configuration?




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

**NEW QUESTION: 18**
Refer to the exhibit. R1 is not forming adjacency on a point-to-point interface. Which action resolves the issue?

R1#show ipv6 ospf neighbor
R1#debug ipv6 ospf hello
OSPFv3 hello events debugging is on
OSPFv3: Rcv hello from 10.1.1.1 area 10 from FastEthernet0/1 FE80::C801:FFF:FE94:1C interface ID 4
OSPFv3: Hello from FE80::C801:FFF:FE94:1C with mismatched NSSA option bit
OSPFv3: Send hello to FF02::5 area 10 on FastEthernet0/1 from FE80::C004:22FF:FE78:1 interface ID 5

Look at the exhibit, R1 is not forming an adjacency on a point to point interface, what can be determined from the debug output and what corrective action is required?

**A.** The area numbers must be configured the same on each router.
**B.** The no-summary command must be included in the area configuration on R2.
**C.** The no-summary command must be included in the area configuration on R1.
**D.** The area types must be configured the same on each router.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 19**
Drag and Drop Question
Drag and drop the LDP features from the left onto the descriptions on the right.

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

**Answer:**

| | |
|---|---|
| | entropy label |
| | implicit null label |
| | explicit null label |
| | inbound label binding filtering |

Explanation:
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: 20**
Refer to the exhibit. An engineer must troubleshoot an issue affecting the communication from router R2 to the TACACS server. Which configuration resolves the issue?

```
*Mar 10 20:13:58.156: AAA/BIND(00000055): Bind i/f
*Mar 10 20:13:58.156: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Mar 10 20:13:58.156: TAC+: Queuing AAA Authentication request 85 for processing
*Mar 10 20:13:58.156: TAC+:(00000055) login timer started 1020 sec timeout
*Mar 10 20:13:58.156: TAC+: processing authentication start request id 85
*Mar 10 20:13:58.156: TAC+: Authentication start packet created for 85()
*Mar 10 20:13:58.156: TAC+: Using server 10.106.60.182
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT: socket event 2
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: Would block while reading
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: read entire 18 bytes response
*Mar 10 20:13:58.156: TAC+:(00000055)/0/225FE2DC: Processing the reply packet
*Mar 10 20:13:58.156: TAC+:: received bad AUTHEN packet: length = 6, expected 43974
*Mar 10 20:13:58.156: TAC+:: Invalid AUTHEN packet (check keys).
```



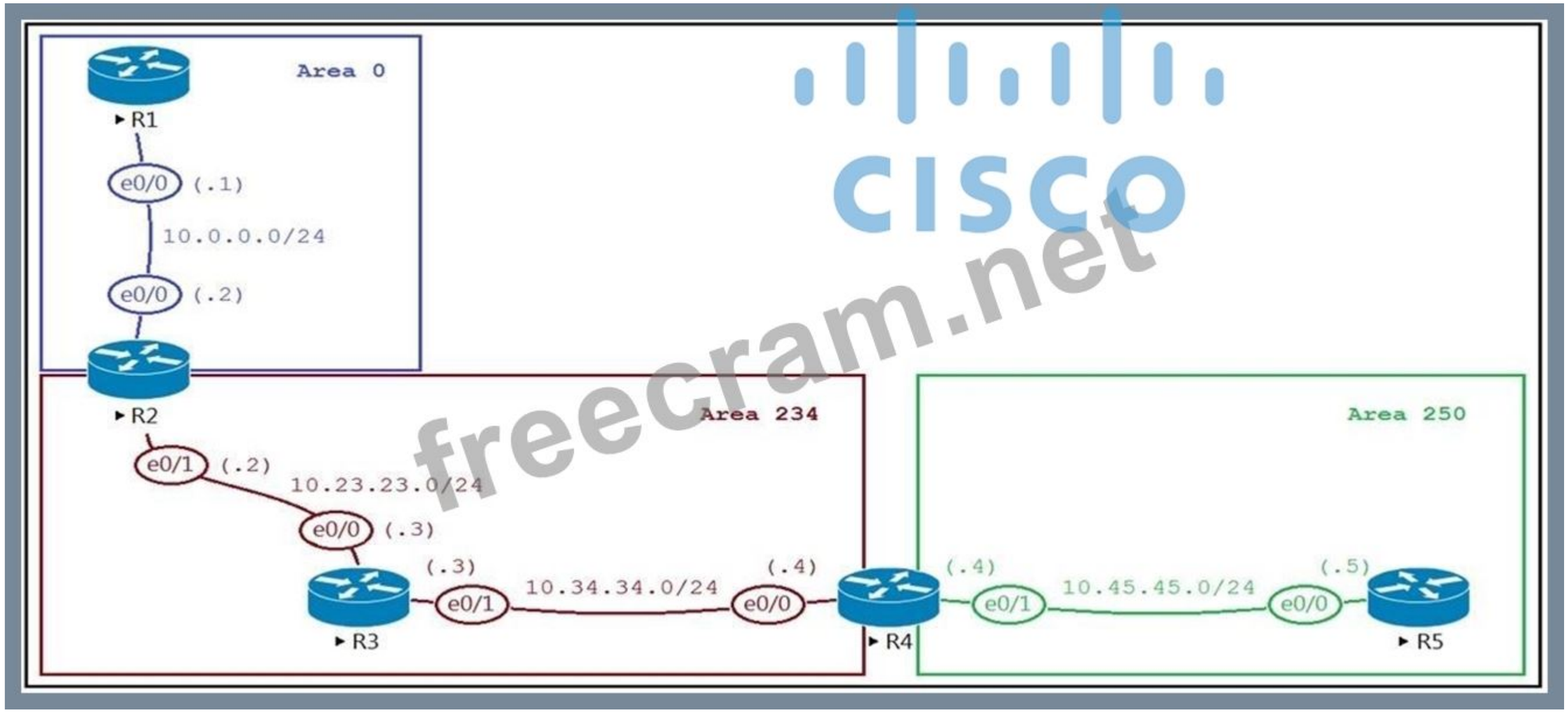
**A.** R1 (config)#tacacs server advrt
R1 (config-server-tacacs)#kty xyz123
**B.** R1 (config)#tacacs-server packet maxsize 43974
**C.** R2(config)#tacacs server advrt
R2 (config-server-tacacs)#key xyz123
**D.** R2(config)#tacacs-server packet maxsize 43974
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 21**
Refer to the exhibit. Which configuration command establishes an EIGRP neighbor adjacency between the hub and spoke?

```
*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
```

**A.** connected 10.1.2.192 command on spoke router
**B.** neighbor 10.1.2.192 command on hub router
**C.** network 10.1.2.192 command on spoke router
**D.** eigrp-peer 10.1.2.192 command on the hub router
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 22**
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.)



**ABR Configurations**

**R2**

```
router ospf 1
 router-id 0.0.0.22
 area 234 virtual-link 10.34.34.4
 network 10.0.0.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 10.22.22.0 0.0.0.255 area 234
 network 10.23.23.0 0.0.0.255 area 234
```

**R4**

```
router ospf 1
 router-id 0.0.0.44
 area 234 virtual-link 10.23.23.2
 network 10.34.34.0 0.0.0.255 area 234
 network 10.44.44.0 0.0.0.255 area 234
 network 10.45.45.0 0.0.0.255 area 250
```

**Virtual Link Status**

```
R4#sh ip ospf virtual-links
Virtual Link OSPF_VL0 to router 10.23.23.2 is down
 Run as demand circuit
 DoNotAge LSA allowed.
 Transit area 234
Topology-MTID  Cost  Disabled  Shutdown  Topology Name
    0         65535  no        no        Base
Transmit Delay is 1 sec, State DOWN,
```



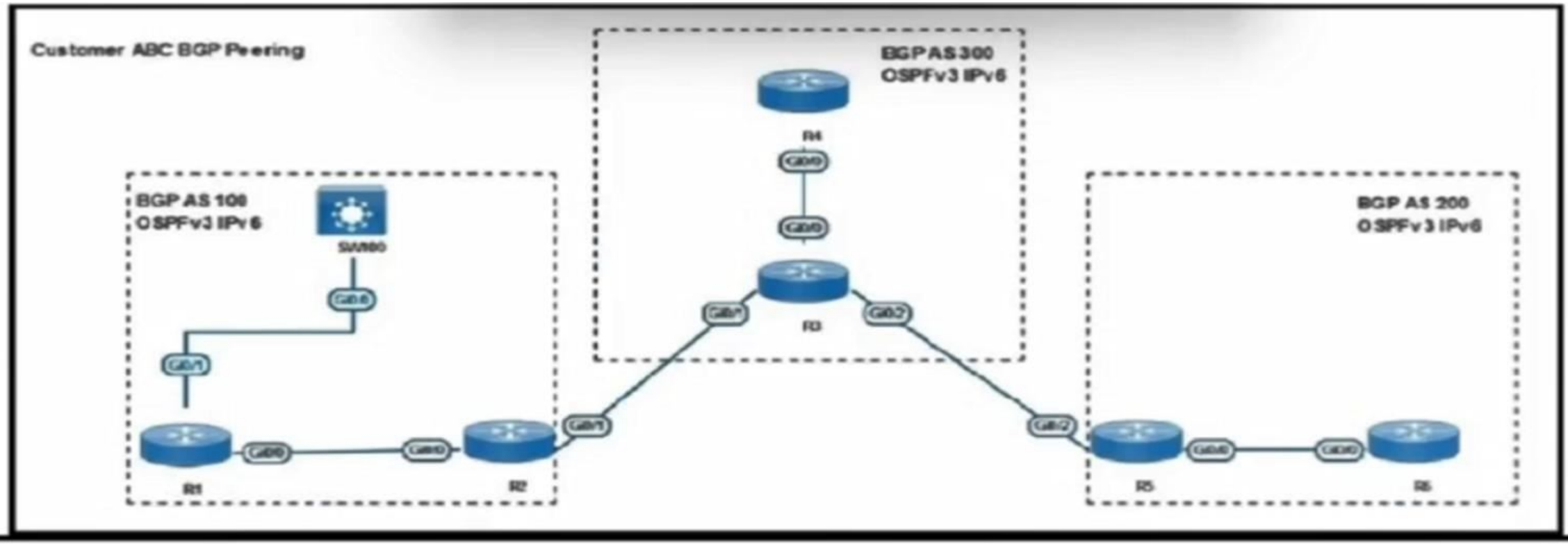
**A.** R4
router ospf 1
no area area 234 virtual-link 10.23.23.2
area 0 virtual-link 0.0.0.22
**B.** R2
router ospf 1
no area area 234 virtual-link 10.34.34.4
area 0 virtual-link 0.0.0.44
**C.** R2
router ospf 1
router-id 10.23.23.2
**D.** R4

router ospf 1
no area 234 virtual-link 10.23.23.2
area 234 virtual-link 0.0.0.22
**E.** R2
router ospf 1
no area 234 virtual-ink 10.34.34.4
area 234 virtual-link 0.0.0.44
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 23**
What TCP port is used by LDP to provide for reliable transport connections?
**A.** 752
**B.** 648
**C.** 712
**D.** 646
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 24**
Which two features are required for MPLS forwarding on which types of routers? (Choose two.)
**A.** CEF on PE and CE routers
**B.** MPLS on PE and core routers
**C.** LDP on PE and CE routers
**D.** LDP on PE and core routers
**E.** MPLS on CE and core routers
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 25**
Refer to the exhibit. R1 cannot reach the R4 loopback address (2001::4/128). Which configuration provides the most optimal and scalable resolution to the issue?

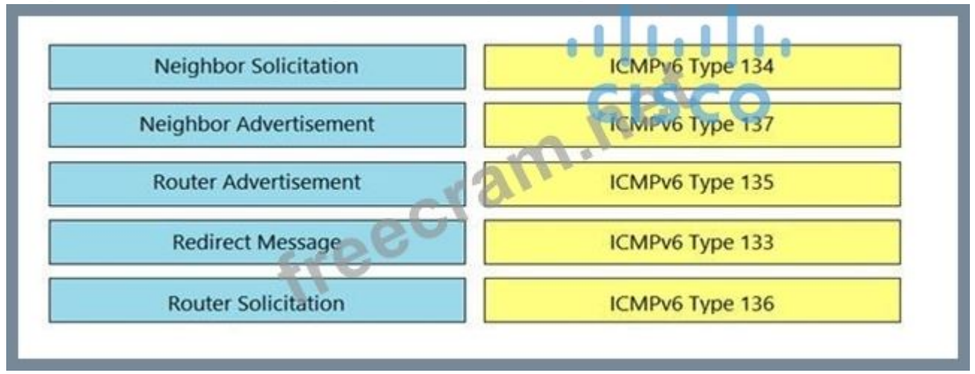



```
R1#sh ip bgp ipv6 unicast
BGP table version is 38, local router ID is 1.1.1.1
     Network          Next Hop            Metric  LocPrf  Weight  Path
 * i  2001::4/128     2001::4                  0     100       0     300 i
 *>i  2002::2/128     2001::2                  0     100       0     i

R1#sh ipv6 route
IPv6 Routing Table - default - 7 entries
C   2001::/64 [0/0]
     via Loopback0, directly connected
L   2001::1/128 [0/0]
     via Loopback0, receive
```

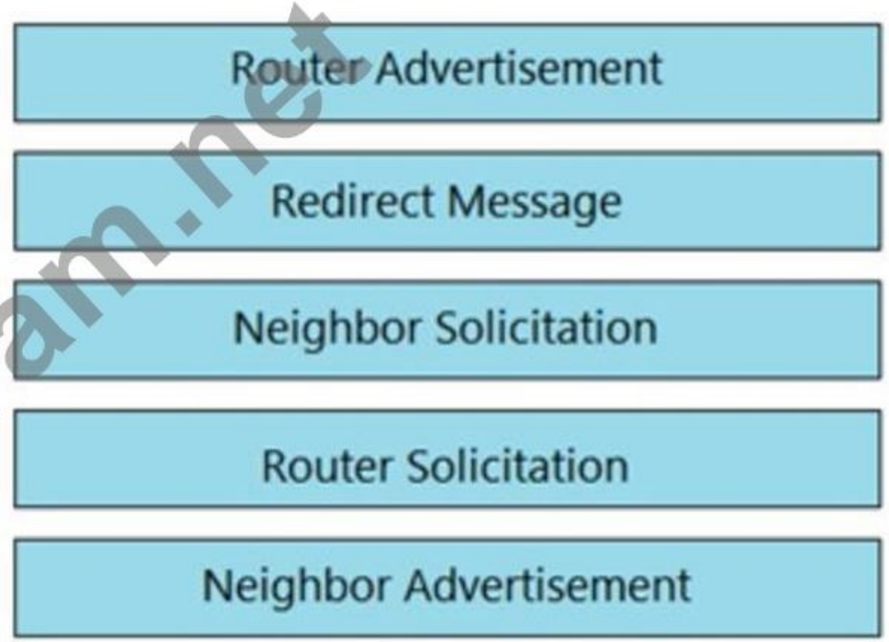
```
O    2001::2/128 [110/1]
      via FE80::5200:C3FF:FE01:E600, GigabitEthernet0/0
C    2001:ABC:AABB:1122::/64 [0/0]
      via GigabitEthernet0/0, directly connected
L    2001:ABC:AABB:1122:1122:1111:2222:AAA1/128 [0/0]
      via GigabitEthernet0/0, receive
B    2002::2/128 [200/0]
      via 2001::2
L    FF00::/8 [0/0]
      via Null0, receive

R1#
```

**A.** R2
router bgp 100
address-family ipv6
neighbor 2001::4 next-hop-self
**B.** R2
router bgp 100
address-family ipv6
no synchronization
**C.** R2
router bgp 100
address-family ipv6
neighbor 2001::4 next-hop-unchanged
redistribute connected
**D.** R1
router bgp 100
address-family ipv6
no synchronization
**Answer: (SHOW ANSWER)**
In the given scenario, R1 cannot reach the R4 loopback address because the next-hop IPv6 address advertised by BGP is not reachable from R1. By default, BGP does not change the next- hop address for routes it advertises to its neighbors. This can cause reachability issues when the next-hop address is not in the same routing domain or not reachable by intermediate routers.
Configuring the next-hop-selfcommand on R2 for the IPv6 BGP neighbor (R1) resolves the issue. This command ensures that R2 advertises itself as the next-hop address to R1 for routes learned from R4. This approach is optimal and scalable because it avoids requiring additional static routes or redistribution configurations.

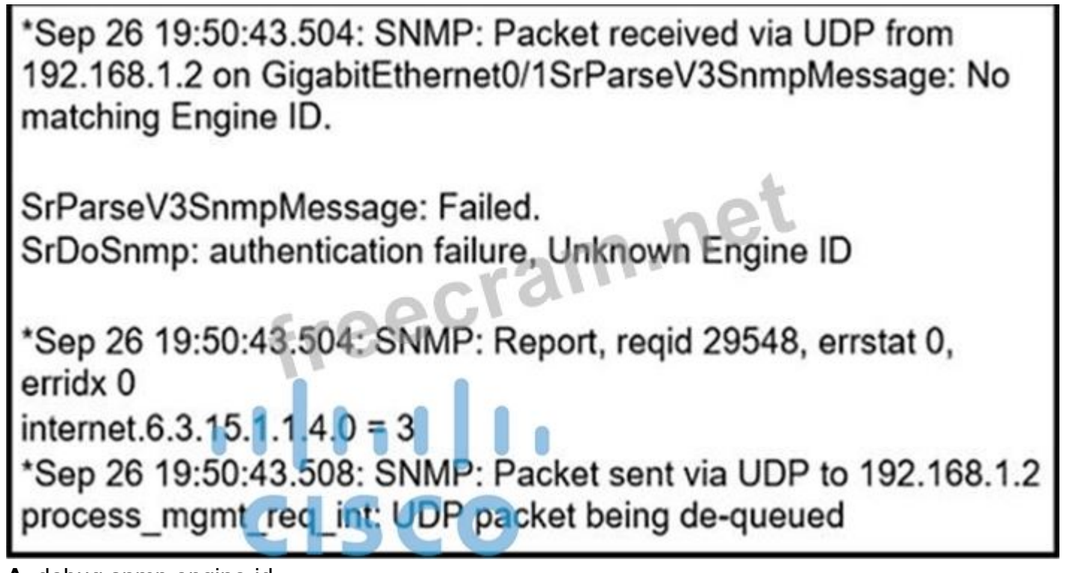
**NEW QUESTION: 26**
Drag and Drop Question
Drag and drop the ICMPv6 neighbor discovery messages from the left onto the correct packet types on the right.




**Answer:**



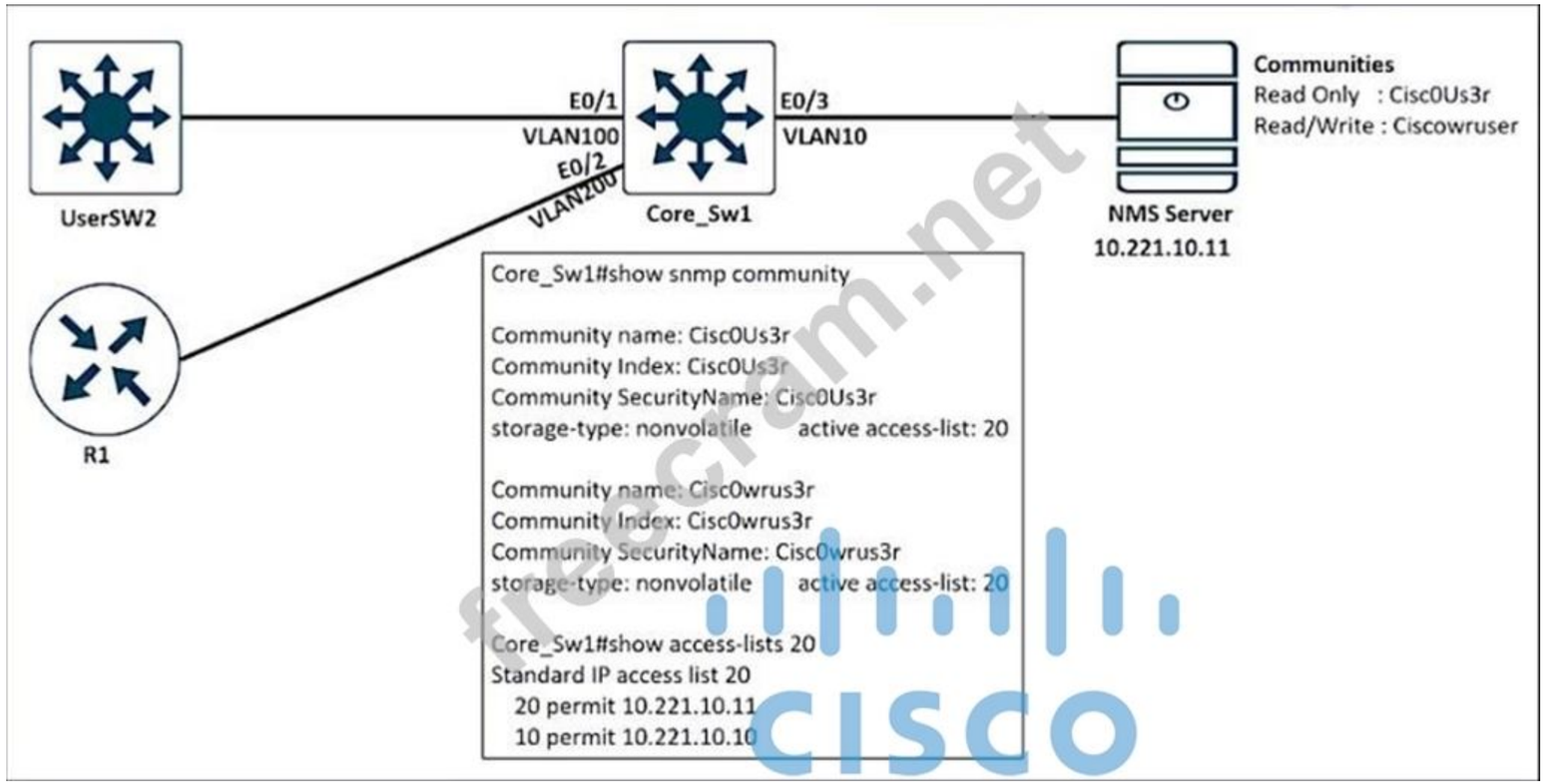

**NEW QUESTION: 27**
Refer to the exhibit. Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)




**A.** debug snmp engine-id
**B.** Show snmp user
**C.** debug snmp packet
**D.** showsnmpv3 user
**E.** debug snmpv3 engine-id

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 28**
Refer to the exhibit. An engineer configured SNMP into Core_Sw1 to be able to upload configurations. When the engineer tried to upload the configuration from the SNMP server, the server failed to log in to the Core Sw1.
Which configuration resolves the issue?




**A.** snmp-server community Cisc0Us3r RW 20

**B.** snmp-server group NETVIEW v2c priv read NETVIEW access 11

**C.** snmp-server community Ciscowruser RW 20

**D.** snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 10

**Answer: (SHOW ANSWER)**

The SNMP server is attempting to upload configurations, which requires Read/Write (RW) access.

According to the exhibit, the community name for Read/Write is Ciscowruser.

Therefore, the correct configuration command is:

snmp-server community Ciscowruser RW 20

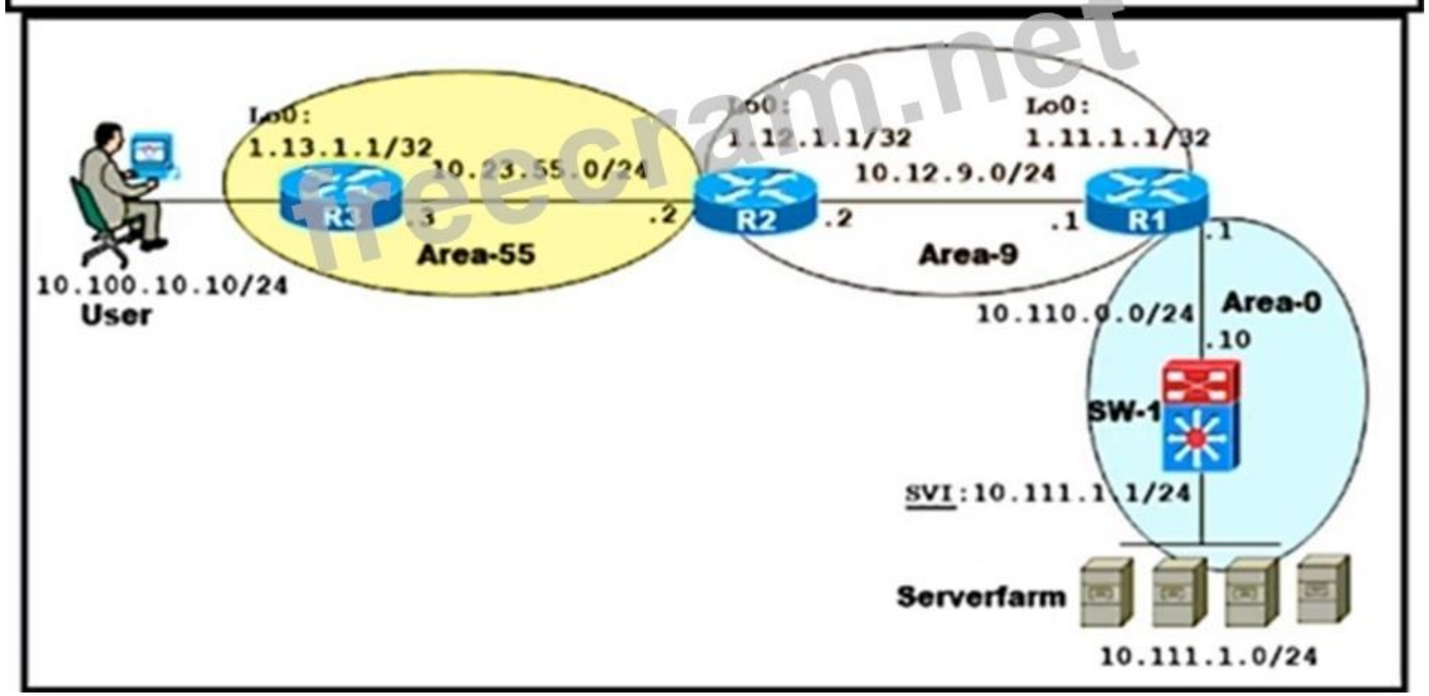
This command allows the SNMP server with the community string Ciscowruser and access list 20 to perform Read/Write operations, which is required to upload configurations.

**NEW QUESTION: 29**

Refer to the exhibit. A user from Area-55 cannot access the HTTPS services running on the Area-

0 server farm. An engineer identifies that the routing table of SW-1 is not learning the Area-55 routes. Which configuration resolves this issue?

```
R5#show ip route

      1.0.0.0/32 is subnetted, 2 subnets
O        1.11.1.1 [110/2] via 10.110.0.1, 00:03:11, GigabitEthernet0/2
O IA     1.12.1.1 [110/3] via 10.110.0.1, 00:03:11, GigabitEthernet0/2
      5.0.0.0/32 is subnetted, 1 subnets
C        5.5.5.5 is directly connected, Loopback0
      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O IA     10.12.9.0/24 [110/2] via 10.110.0.1, 00:03:11, GigabitEthernet0/2
C        10.110.0.0/24 is directly connected, GigabitEthernet0/2
L        10.110.0.5/32 is directly connected, GigabitEthernet0/2
C        10.111.1.0/24 is directly connected, GigabitEthernet0/0
L        10.111.1.1/32 is directly connected, GigabitEthernet0/0
```




**A.** R1
router ospf 100
area 9 virtual-link 10.12.9.1
R3
router ospf 100
area 9 virtual-link 1.23.55.2

**B.** R1
router ospf 100
area 9 virtual-link 10.110.0.1
R2

router ospf 100
area 9 virtual-link 1.12.9.1
**C.** R3
router ospf 100
area 9 virtual-link 1.13.1.1
R1
router ospf 100
area 9 virtual-link 1.12.1.1
**D.** R2
router ospf 100
area 9 virtual-link 1.11.1.1
R1
router ospf 100
area 9 virtual-link 1.12.1.1
**Answer: (SHOW ANSWER)**
In OSPF, all non-backbone areas (non-Area 0) must have a direct connection to Area 0, either physically or logically through a virtual link. In this topology:
- Area 55 connects to Area 9 through R3 → R2.
- Area 9 connects to Area 0 through R2 → R1.
- However, Area 9 is not directly connected to Area 0, and there's no virtual link configured.
As a result, Area 55 routes are not being advertised to Area 0, and SW1 doesn't learn the routes to reach the user in Area 55.
To resolve this, a virtual link between R2 and R1 through Area 9 is needed. This logically connects Area 9 to Area 0, allowing OSPF to pass routing information between them.
The virtual link must be configured using router IDs of R1 and R2 (1.11.1.1 and 1.12.1.1), and Area 9 as the transit area.

**NEW QUESTION: 30**
Refer to the exhibit. An engineer must filter incoming EIGRP updates to allow only a set of specific prefixes. The distribute list is tested, and it filters out all routes except network 10.10.10.0/24. How should the engineer temporarily allow all prefixes to be learned by the router again without adjusting the existing access list?

```
R1(config) #ip access-list standard EIGRP-FILTER
R1(config-std-nacl) #permit 10.10.10.0 0.0.0.255
R1(config) #router eigrp 10
R1(config-router) #distribute-list route-map EIGRP in
!
R1(config) #route-map EIGRP permit 10
R1(config-route-map) #match ip address EIGRP-FILTER
!
R1#show ip route eigrp
D     10.10.10.0/24
```

**A.** A permit 20 statement should be added before completing the ACL with the required prefixes, and then the permit 20 statement can be removed.
**B.** A permit any statement should be added before completing the ACL with the required prefixes and then the permit any statement can be removed.
**C.** A continue statement should be added within the permit 10 statement before completing the ACL with the required prefixes, and then the continue statement can be removed.
**D.** An extended access list must be used instead of a standard access list to accomplish the task
**Answer: (SHOW ANSWER)**
To temporarily allow all prefixes without modifying or deleting the existing filter (which currently only permits 10.10.10.0/24), the engineer can add a second permitstatement to the access list (e.g., permit anyor a broader

range) with a higher sequence number, such as 20.
This allows all routes temporarily, and later, the permit 20line can be removed once the required prefixes are ready to be configured.
This avoids touching the existing permit 10statement and maintains structured control of route filtering.

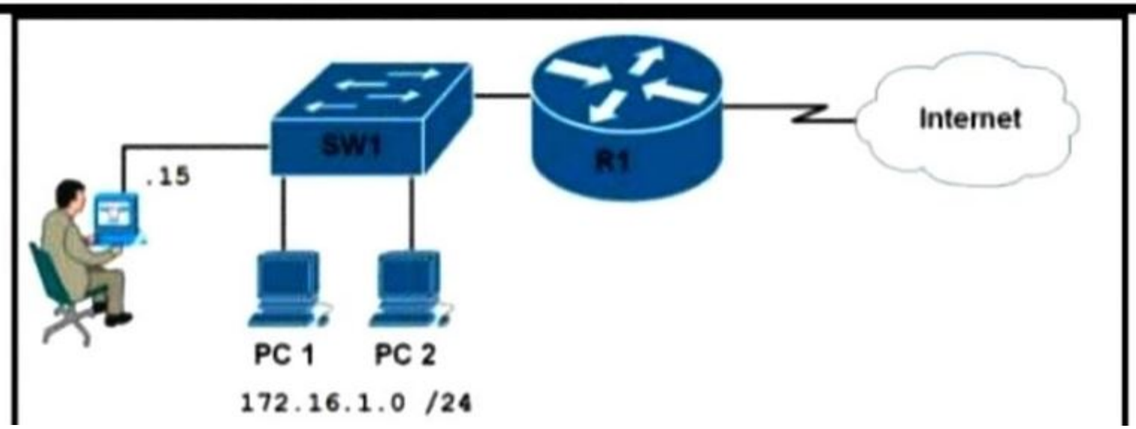
**NEW QUESTION: 31**
What is a function of IPv6 Source Guard?
**A.** It notifies the ND protocol to inform hosts if the traffic is denied by it.
**B.** It works with address glean or ND to find existing addresses.
**C.** It denies traffic from known sources and allocated addresses.
**D.** It inspects ND and DHCP packets to build an address binding table.
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 32**
Refer to the exhibit. After a RADIUS server fails AAA authentication, an engineer is trying to reestablish console access to a switch using the local password.
Which configuration reestablishes the console access to switch SW1 via AAA?

```
R1#sh run | begin ip forward
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 15 permit 172.16.1.15
!
control-plane
!
line con 0
```

```
line aux 0
line vty 0 4
 exec-timeout 0 1
 login authentication CCNP
 transport input all
!
```




**A.**
```
SW1(config)#aaa authentication login CONSOLE line
SW1(config)#username ENT secret QZsek239@
SW1(config)#line con 0
SW1(config-line)#login authentication CONSOLE
```

**B.**
```
SW1(config)#aaa authentication login CONSOLE local
SW1(config)#username ENT secret QZsek239@
SW1(config)#line con 0
SW1(config-line)#login authentication CONSOLE
```

**C.**
```
SW1(config)#aaa authentication login CONSOLE local
SW1(config)#username ENT password 7 QZsek239@
SW1(config)#line con 0
SW1(config-line)#login authentication CONSOLE
```

**D.**
```
SW1(config)#aaa authentication login CONSOLE line
SW1(config)#username ENT password 7 QZsek239@
SW1(config)#line con 0
SW1(config-line)#login authentication CONSOLE
```

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 33**

A network administrator successfully established a DMVPN tunnel with one hub and two spokes using EIGRP. One of the requirements was to enable spoke-to-spoke tunnels through the hub router using EIGRP. Which configuration command must the engineer configure to meet the requirement?

**A.** no ip eigrp 1 split-horizon
**B.** no ip eigrp 1 mode mgre
**C.** no ip eigrp 1 tunnel-redirect
**D.** no ip eigrp 1 mode multipoint
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 34**
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?

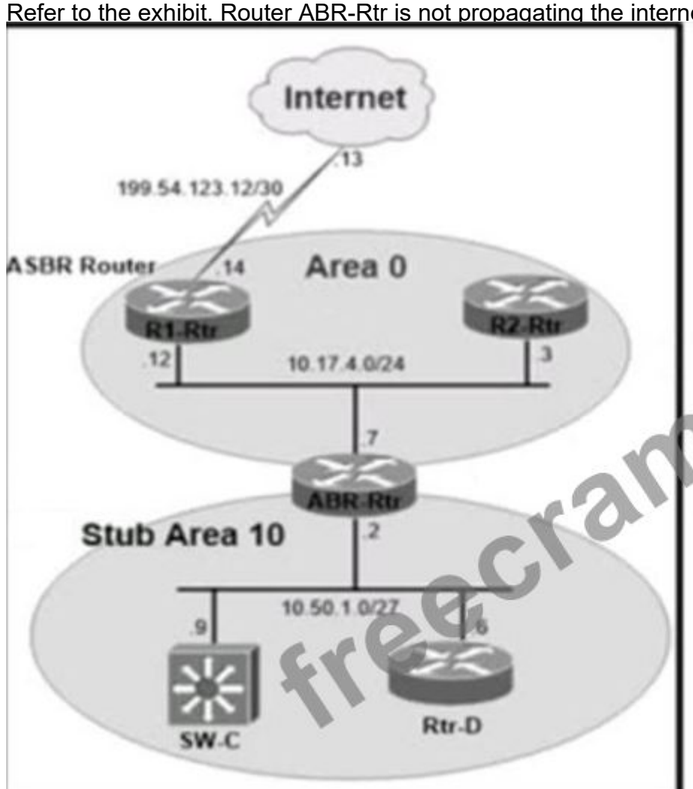
```
CPE# ping 10.0.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.4, timeout is
2seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
=1/1/1 ms
CPE# copy flash:/packages.conf tftp://10.0.2.4/
Address or name of remote host [10.0.2.4]?
Destination filename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



**A.** Make the packages.conf file executable by all on the TFTP server
**B.** Make the packages.conf file writable by all on the TFTP server
**C.** Make sure to run the TFTP service on the TFTP server
**D.** Make the TFTP folder writable by all on the TFTP server
**Answer: (SHOW ANSWER)**
During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

**NEW QUESTION: 35**
Which IGPs are supported by the MPLS LDP autoconfiguration feature?
**A.** ISIS and RIPv2
**B.** RIPv2 and OSPF
**C.** OSPF and ISIS
**D.** OSPF and EIGRP
**Answer: (SHOW ANSWER)**
The MPLS LDP Autoconfiguration feature enables you to globally enable LDP on every interface associated with an IGP instance. This feature is supported on OSPF and IS-IS IGPs. It provides a means to block LDP from being enabled on interfaces that you do not want enabled.
Reference: https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/convert/mp_ldp_ book/mp_ldp_autoconfig.html

**NEW QUESTION: 36**
Refer to the exhibit. Router ABR-Rtr is not propagating the internet routes in OSPF area 10 which causes internet reachability problems in the area. Which action resolves the issue?




**R1-Rtr Configuration:**

```
router ospf 1
log-adjacency-changes
network 10.17.4.12 0.0.0.0 area 0
default information originate
!
ip route 0.0.0.0 0.0.0.0 199.54.123.13
!
```

**ABR-Rtr Configuration:**

```
router ospf 1
log-adjacency-changes
network 10.50.1.2 0.0.0.0 area 10
area 10 stub
```

**SW-C Configuration:**

```
router ospf 1
log-adjacency-changes
network 10.50.1.9 0.0.0.0 area 10
area 10 stub
```

**Rtr-D Configuration:**

```
router ospf 1
log-adjacency-changes
network 10.50.1.6 0.0.0.0 area 10
area 10 stub
```



**A.** ABR-Rtr must advertise the 0.0.0.0/0 default route in area 10.
**B.** ABR-Rtr must configure the area 10 stub no-summary command.
**C.** ABR-Rtr must configure the default-information originate always command.
**D.** ABR-Rtr network type must be broadcast network.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 37**
The MPLS LDP autoconfiguration feature allows you to enable LDP on every interface that is associated with an IGP instance. Which of the following Interior Gateway Protocols support this? (Choose two.)
**A.** BGP
**B.** RIP
**C.** OSPF

**D.** IS-IS
**E.** EIGRP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 38**
Unicast Reverse Path Forwarding (uRPF) has been configured on a service provider network to protect itself from spoofed based attacks. Which of the following are valid uRPF modes? (Choose two.)
**A.** Closed mode
**B.** Loose mode
**C.** Strict mode
**D.** Block mode
**E.** Open mode
**Answer: (SHOW ANSWER)**

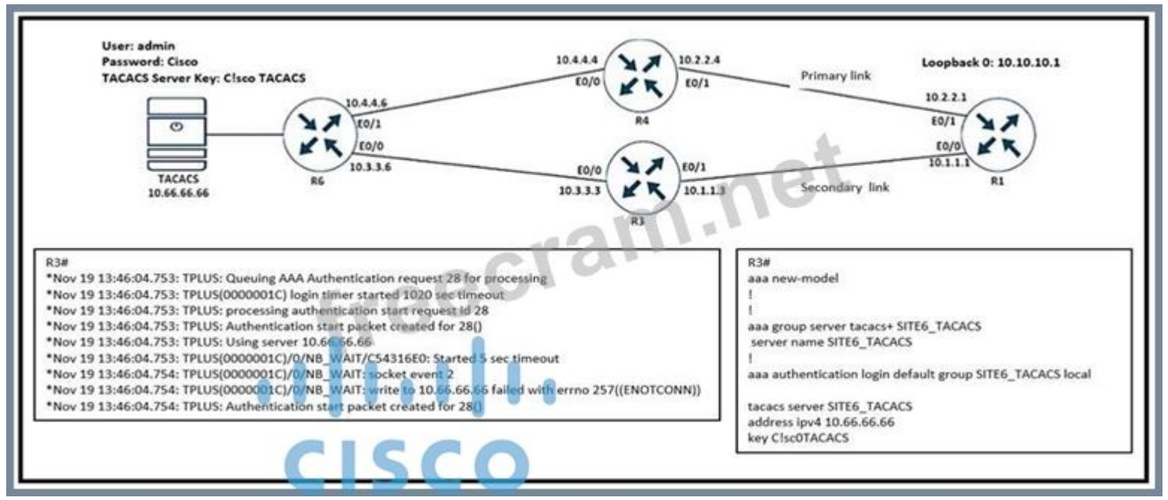
**NEW QUESTION: 39**
The network administrator configured the router for Control Plane Policing so that inbound SSH traffic is policed to 500 kbps. This policy must apply to traffic coming in from 10.10.10.0/24 and 192.168.10.0/24 networks.
access-list 100 permit ip 10.10.10.0 0.0.0.255 any
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 23
!
class-map CLASS-SSH
match access-group 100
!
policy-map PM-COPP
class CLASS-SSH
police 500000 conform-action transmit
!
interface E0/0
service-policy input PM-COPP
!
interface E0/1
service-policy input PM-COPP
The Control Plane Policing is not applied to SSH traffic and SSH is open to use any bandwidth available. Which configuration resolves this issue?
**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
!
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
**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
!
policy-map PM-COPP
class CLASS-SSH
no police 500000 conform-action transmit
police 500000 conform-action transmit exceed-action drop
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 40**
An engineer configured a Cisco router to send reliable and encrypted notifications for any events to the management server.
It was noticed that the notification messages are reliable but not encrypted.
Which action resolves the issue?

**A.** Configure all devices for SNMPv3 informs with priv.
**B.** Configure all devices for SNMPv3 informs with auth.
**C.** Configure all devices for SNMPv3 traps with auth.
**D.** Configure all devices for SNMPv3 traps with priv.
**Answer: (SHOW ANSWER)**
SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when this device receives traps."Send reliable and encrypted notifications for any events" so it is SNMP notifications. For encryption we need to configure "priv".

**NEW QUESTION: 41**
Refer to the exhibit R3 cannot authenticate via TACACS. Which configuration resolves the issue?




**A.** tacacs server SITE6_TACACS
key C!sc0TACACS
**B.** tacacs server SITE6_TACACS
key C!scoTACACS
**C.** tacacs server SITE6_TACACS
address ipv4 10.60.66.66
key C!scoTACACS
**D.** tacacs server SITE6_TACACS
address ipv4 10.66.66.66
key CiscoTACACS
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 42**
Refer to the exhibit. Routers R1 and R2 exchange routes to each other's loopback through OSPF. Telnet traffic must be blocked from R2 Lo0 to R1 Lo2. Which configuration resolves the issue?

R1

```
Interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
ipv6 traffic-filter DENY_TELNET_Lo2 in
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

```
R1
interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 traffic-filter DENY_TELNET_Lo2 in
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telne
 permit ipv6 any any
```

A.

```
R1
interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

B.

```
interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
ipv6 access-class DENY_TELNET_Lo2 in
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

C.

R1

```
interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 access-class DENY_TELNET_Lo2 in
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

**D.**

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 43**

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

```
R1#sh ip route

     192.168.10.0/24 is directly connected, Serial1/0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 mask
        172.16.160.0/19 is directly connected, Loopback1
        172.16.128.0/19 is directly connected, Loopback0
        172.16.224.0/19 is directly connected, Loopback3
        172.16.192.0/19 is directly connected, Loopback2
        172.16.0.0/16 is a summary, 00:01:27, Null0
```

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

**B.** R1#configure terminal
R1 (config)#router BGP 100
R1 (config-router)#auto-summary
**C.** R2#configure terminal
R2 (config)#router BGP 100
R2 (config-router)#no auto-summary
**D.** R1#configure terminal
R1 (config)#router BGP 100
R1 (config-router)#no auto-summary
**Answer: (SHOW ANSWER)**
By default, BGP performs automatic summarization of routes at classful boundaries. If specific subnets need to be advertised instead of a single summary route (e.g., 172.16.0.0/16), the no auto-summary command should be applied on the router originating the routes (R2 in this case).
Applying no auto-summary ensures that R2 advertises the more specific subnets (e.g.,
172.16.128.0/19, 172.16.160.0/19, etc.) to R1 without summarizing them into the single
172.16.0.0/16 route.

**NEW QUESTION: 44**
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)**
IPv6 Source Guard filters inbound traffic on L2 switch ports that are not in the IPv6 binding table.
The binding table stores the following information:
+ IPv6 address
+ MAC address
+ VLAN
+ Interface ID

**NEW QUESTION: 45**
Refer to the exhibit. An engineer troubleshoots a connectivity problem that is impacting the communication from the users at segment 172.16.3.16 /28 to the server farm at 192.168.5.16/28.
Which configuration resolves the issue on router R1?

```
R4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C        172.16.3.0/30 is directly connected, GigabitEthernet0/3
L        172.16.3.2/32 is directly connected, GigabitEthernet0/3
C        172.16.3.16/28 is directly connected, Loopback0
L        172.16.3.17/32 is directly connected, Loopback0
C        172.16.3.32/28 is directly connected, Loopback1
L        172.16.3.33/32 is directly connected, Loopback1
R        172.16.250.0/30 [120/1] via 172.16.3.1, 00:00:04, GigabitEthernet0/3
R        172.16.250.12/30 [120/1] via 172.16.3.1, 00:00:04, GigabitEthernet0/3
R4#
```

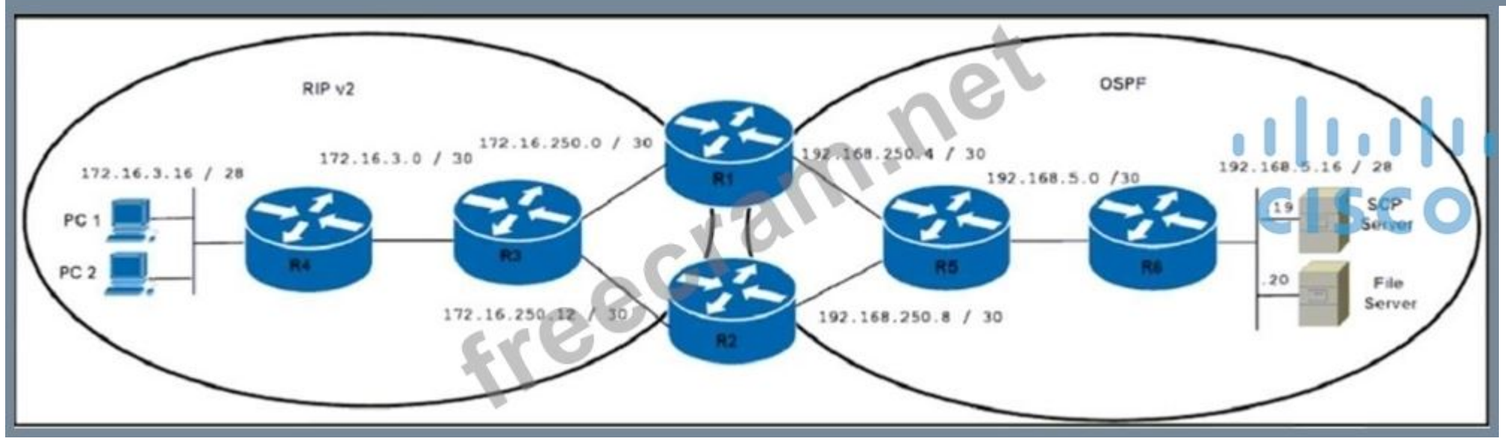
```
R3#sho ip route
Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
S        10.2.0.0 is directly connected, Null0
      172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C        172.16.3.0/30 is directly connected, GigabitEthernet0/3
L        172.16.3.1/32 is directly connected, GigabitEthernet0/3
R        172.16.3.16/28 [120/1] via 172.16.3.2, 00:00:17, GigabitEthernet0/3
R        172.16.3.32/28 [120/1] via 172.16.3.2, 00:00:17, GigabitEthernet0/3
C        172.16.250.0/30 is directly connected, GigabitEthernet0/1
L        172.16.250.2/32 is directly connected, GigabitEthernet0/1
C        172.16.250.12/30 is directly connected, GigabitEthernet0/2
L        172.16.250.14/32 is directly connected, GigabitEthernet0/2
R     192.168.5.0/24 [120/15] via 172.16.250.13, 00:00:10, GigabitEthernet0/2
R     192.168.250.0/24
           [120/15] via 172.16.250.13, 00:00:10, GigabitEthernet0/2
R3#
```

```
R1#show running-config | begin router ospf 1
router ospf 1
 redistribute rip subnets
 network 192.168.250.0 0.0.0.255 area 0
!
router rip
 version 2
 redistribute ospf 1 metric 15
 network 172.16.0.0
!
```

```
R2#show run | begin router ospf
router ospf 1
 redistribute rip subnets
 network 192.168.250.0 0.0.0.255 area 0
!
router rip
 version 2
 redistribute ospf 1 metric 15
 network 172.16.0.0
!
```

```
R3#traceroute 192.168.5.17
Type escape sequence to abort.
Tracing the route to 192.168.5.17
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.250.1 15 msec
    172.16.250.13 13 msec
    172.16.250.1 26 msec
  2 192.168.250.10 29 msec
    192.168.250.5 42 msec
    192.168.250.10 13 msec
  3 192.168.5.2 50 msec 27 msec *
R3#
```

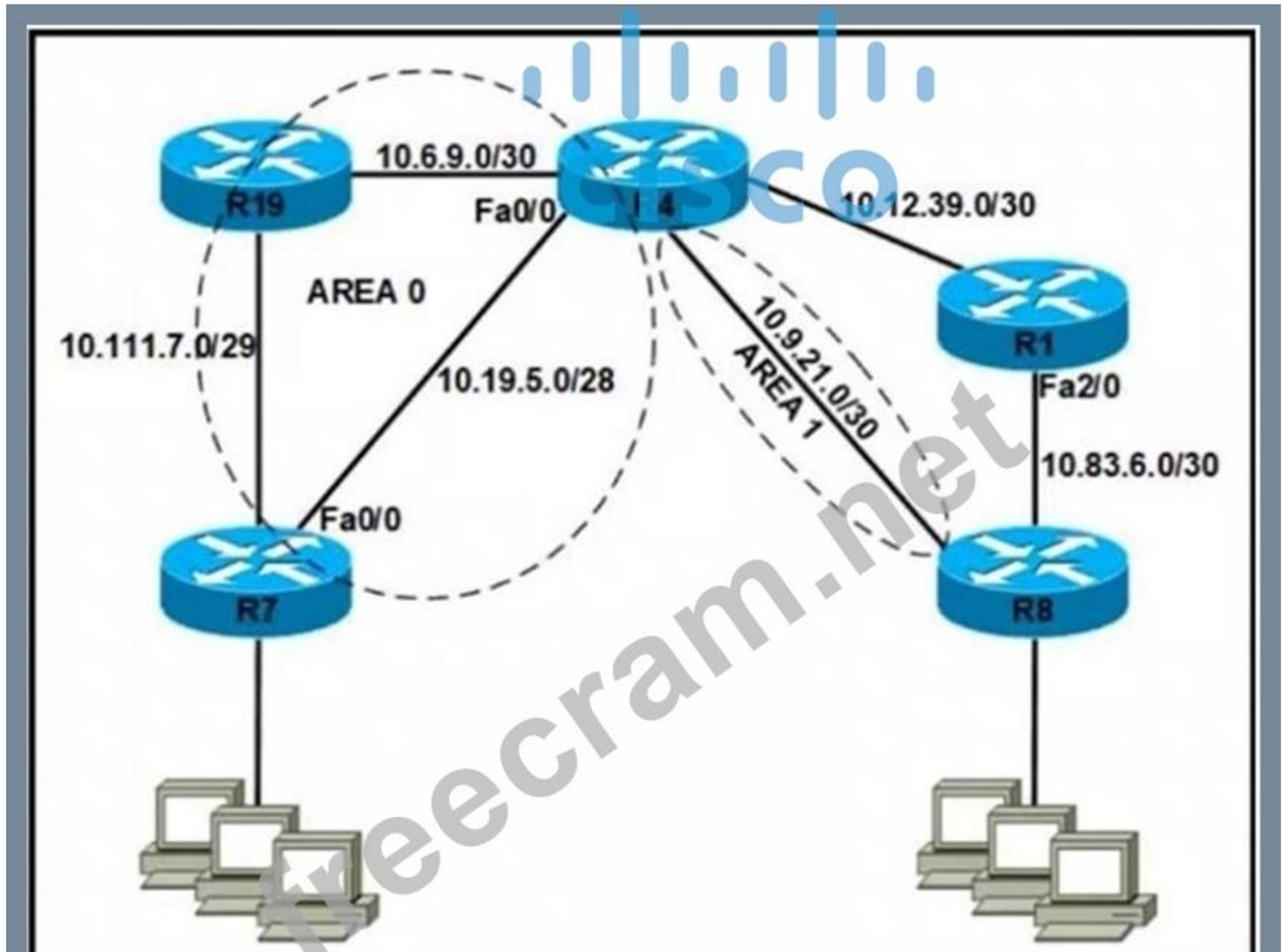
```
R4#traceroute 192.168.5.17
Type escape sequence to abort.
Tracing the route to 192.168.5.17
VRF info: (vrf in name/id, vrf out name/id)
  1  *  *  *
  2  *  *  *
  3  *  *  *
  4  *  *  *
R4#
```




**A.** router ospf 1
redistribute rip metric 16
**B.** router rip
redistribute ospf 1 metric 14
**C.** router rip
redistribute ospf 1 metric 16

**D.** router ospf 1
redistribute rip metric 14
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 46**
Refer to the exhibit. Router R4 is configured correctly with default OSPF values. A network engineer configured R7 for OSPF. R7 must not be elected as a DR for the segment between R4- R7. The adjacency between R4 and R7 failed to form.
Which configuration resolves the issue?




```
R7#sh ip ospf interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 10.19.5.2/28, Area 0, Attached via Network Statement
  Process ID 1, Router ID 10.7.7.255, Network Type POINT_TO_POINT, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1          no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 15, Wait 15, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
```

A.
```
R7(config)#interface fa0/0
R7(config-if)#ip ospf priority 0
R7(config-if)#ip ospf hello-interval 10
R7(config-if)#ip ospf dead-interval 30
R7(config-if)#ip ospf network non-broadcast
```

B.
```
R7(config)#interface fa0/0
R7(config-if)#ip ospf priority 255
R7(config-if)#ip ospf hello-interval 10
R7(config-if)#ip ospf dead-interval 40
R7(config-if)#ip ospf network non-broadcast
```

C.
```
R7(config)#interface fa0/0
R7(config-if)#ip ospf priority 0
R7(config-if)#ip ospf hello-interval 10
R7(config-if)#ip ospf dead-interval 40
R7(config-if)#ip ospf network broadcast
```

D.
```
R7(config)#interface fa0/0
R7(config-if)#ip ospf priority 255
R7(config-if)#ip ospf hello-interval 10
R7(config-if)#ip ospf dead-interval 30
R7(config-if)#ip ospf network broadcast
```

**Answer: (SHOW ANSWER)**



**NEW QUESTION: 47**

Refer to the exhibit. A user cannot SSH to the router.

What action must be taken to resolve this issue?

```
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.** Configure transport input ssh
**B.** Configure transport output ssh
**C.** Configure ip ssh version 2
**D.** Configure ip ssh source-interface loopback0

**Answer: (SHOW ANSWER)**

On Cisco IOS the VTY lines default to accepting Telnet only. Even after you've created RSA keys and a local user database, you must explicitly enable SSH on the VTYs. Under line vty 0 15 add transport input ssh.

This switches the VTYs from Telnet to SSH, allowing SSH logins.

**NEW QUESTION: 48**
Refer to the exhibit. The server for the finance department is not reachable consistently on the 200.30.40.0/24 network and after every second month it gets a new IP address.

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



Which two actions must be taken to resolve this Issue? (Choose two.)
**A.** Configure the server to use DHCP on the network with default gateway 200 30.40.100.
**B.** Configure the server with a static IP address and default gateway.
**C.** Configure the router to exclude a server IP address.
**D.** Configure the server to use DHCP on the network with default gateway 200 30.30.100.
**E.** Configure the router to exclude a server IP address and default gateway.
**Answer: (SHOW ANSWER)**
The command "lease 40" set the duration of the lease (the time during which a client computer can use an assigned IP address). The syntax is "lease {days[hours] [minutes] | infinite}". In this case the lease is 40 days. Therefore the server for the finance department is getting new IP address every 40 days. It is very inconvenient and we should assign/configure a static IP address for the finance department server. We can do it via two ways:
+ Static configure an IP address on the finance department server and exclude that IP address in the DHCP pool
+ Instruct the DHCP pool to assign a specific IP address for the MAC address of the finance department server (via the "client-identifier ..." or "hardware-address ..." command)

**NEW QUESTION: 49**
Which location within the network is preferred when using a dedicated route for Cisco IP SLA operations?
**A.** access edge
**B.** distribution edge
**C.** provider edge
**D.** user edge

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 50**

What is the purpose of the DHCPv6 Guard?

**A.** It shows that clients of a DHCPv6 server are affected.

**B.** It messages between a DHCPv6 server and a DHCPv6 client (or relay agent).

**C.** It blocks DHCPv6 messages from relay agents to a DHCPv6 server.

**D.** It allows DHCPv6 reply and advertisements from (rogue) DHCPv6 servers.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 51**

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-router)#ospfv3 3 1

**D.** Router# ospfv3 1 address-family ipv4 unicast

**Answer: (SHOW ANSWER)**

The newest OSPFv3 configuration approach utilizes a single OSPFv3 process. It is capable of supporting IPv4 and IPv6 within a single OSPFv3 process. OSPFv3 builds a single database with LSAs that carry IPv4 and IPv6 information. The OSPF adjacencies are established separately for each address family. Settings that are specific to an address family (IPv4/IPv6) are configured inside that address family router configuration mode.

Running single OSPFv3 for both IPv4 and IPv6 is supported since Cisco IOS Software Release
15.1(3)S.

The new-style OSPFv3 process is enabled using the router ospfv3 process-number command.

Within the OSPF process configuration mode, the OSPF process ID is defined (using the router- id ospf-process-ID command).

OSPFv3 New-Style OSPF Configuration Commands:

```
R1(config)#ipv6 unicast-routing //although only OSPFv3 for IPv4 is configured but we have to enable IPv6 under global
configuration mode
R1(config)#router ospfv3 1
R1(config-router)# router-id 1.1.1.1
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ipv6 enable //although only OSPFv3 for IPv4 is configured but we have to enable IPv6 under interface
mode
R1(config-if)#ospfv3 1 ipv4 area 0
```

Therefore answer B is the best answer here but in this answer, the configuration mode is not correct. It should be interface mode (config-if)#, not router mode (config-router)#.

Reference: https://www.ciscopress.com/articles/article.asp?p=2294214&seqNum=4

**NEW QUESTION: 52**

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?

```
R1# show ip route static
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
S       10.100.13.0/24 is directly connected, Loopback10
R1# show run | begin router ospf 1
router ospf 1
 redistribute static
 network 10.100.11.0 0.0.0.255 area 1
 network 10.100.12.0 0.0.0.255 area 1
 network 10.100.14.0 0.0.0.255 area 1

R2# show ip route 10.100.13.0
% Subnet not in table
R2# show ip ospf neighbor | include 10.100.14.1
10.100.14.1      1   FULL/DR         00:00:39    10.100.14.1
GigabitEthernet0/0
```

**A.** The redistribution command is incorrect on R1. The default metric metric 200 should be inducted with the redistribution command.

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

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

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

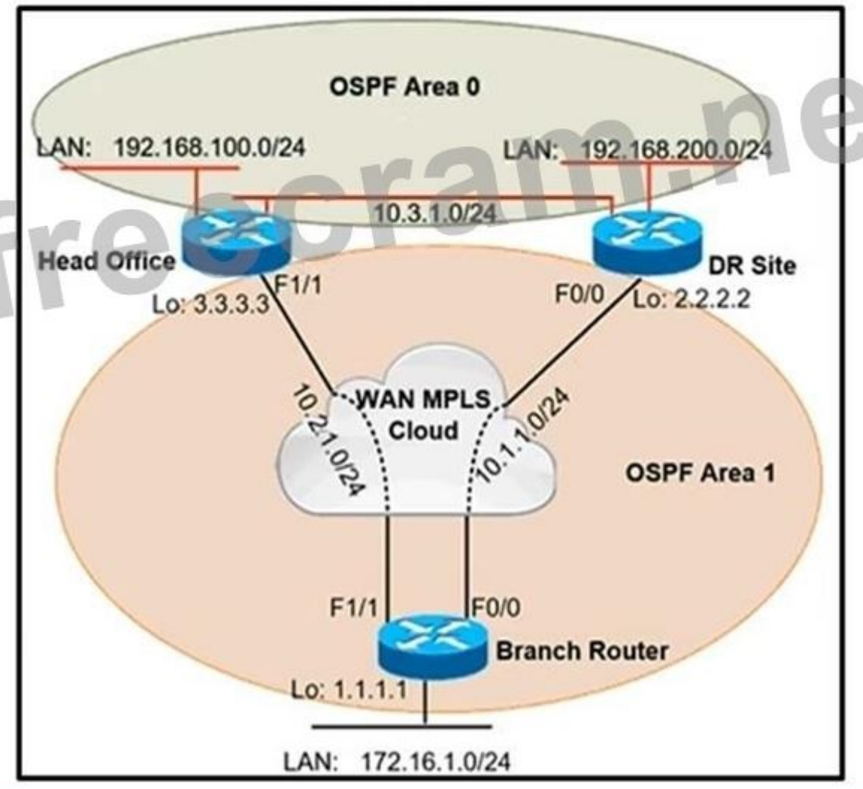
**Answer: D (LEAVE A REPLY)**

In OSPF, when redistributing static routes, the subnets keyword is required to ensure that OSPF redistributes all subnets, including those with subnet masks (e.g., /24). Without the subnets keyword, OSPF will only redistribute classful networks, which may exclude subnets like
10.100.13.0/24.
To resolve the issue, update the OSPF configuration on R1 to include the subnets keyword:
router ospf 1
redistribute static subnets
This ensures that the static route for 10.100.13.0/24 is correctly redistributed into OSPF and propagated to R2.

**NEW QUESTION: 53**

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?

```
Branch-Router#
"Nov 29 15.20.22.415: OSPF-1 HELLO Fa1/1: Rcv hello from 3.3.3.3 area 1 10.2.1.3
"Nov 29 15.20.23.195: OSPF-1 HELLO Fa1/1: Send hello to 224.0.0.5 area 1 from 10.2.1.1

Branch-Router#
"Nov 29 15.20:27.955: OSPF-1 HELLO Fa0/0: Rcv hello from 2.2.2.2 area 1 10.1.1.2
"Nov 29 15.20.27.955: OSPF-1 HELLO Fa0/0: Mismatched hello parameters from 10.1.1.2
"Nov 29 15.20.27.955: OSPF-1 HELLO Fa0/0: Dead R 40 C 40, Hello R 10 C 10 Mask R 255.255.255.0 C 255.255.255.240
"Nov 29 15.20.28.311: OSPF-1 HELLO Fa0/0: Send hello to 224.0.0.5 area 1 from 10.1.1.1
```




**A.** Advertise the branch WAN interface matching subnet for the DR site.

**B.** Configure matching hello and dead intervals between sites.

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

**D.** Stabilize the DR site flapping link to establish OSPF adjacency.

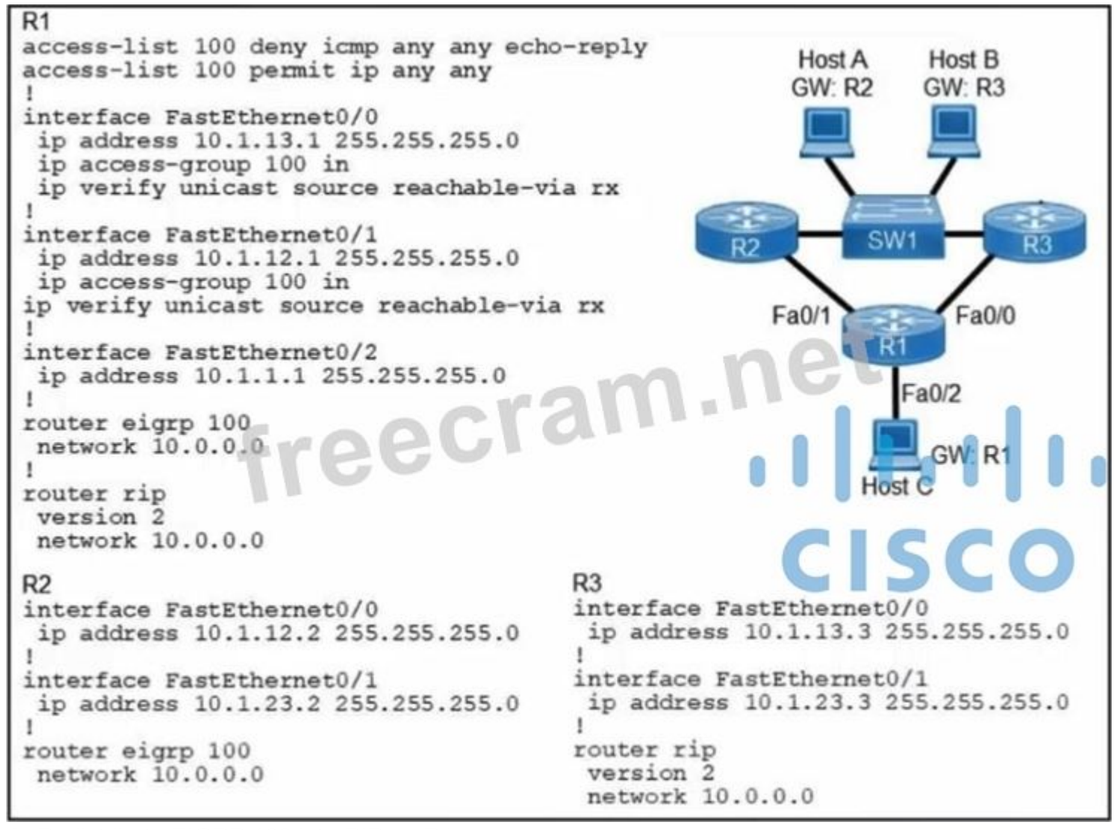
**Answer: (SHOW ANSWER)**

The netmask doesn't match between neighbors

R1#

OSPF: Mismatched hello parameters from 192.168.12.2
OSPF: Dead R 40 C 40, Hello R 10 C 10 Mask R 255.255.255.128 C 255.255.255.0 Now we have something to work with. R1 says it received a hello packet but we have mismatched hello parameters. The R stands for what we received and the C stands for what we have configured.
You can see that there is a mismatch in the subnet mask. R1 is configured with subnet mask
255.255.255.0 while R2 has subnet mask 255.255.255.240. OSPF will only compare the subnet mask when you are using the broadcast network type. You can also spot this error if you look at the OSPF information per interface. Broadcast is using a DR router while point-to-point doesn't use a DR router.

**NEW QUESTION: 54**
Refer to the exhibit. Host A successfully pings host C, but host B fails to ping host C. Which action resolves this issue?




**A.** Redistribute EIGRP 100 into RIP on R1.
**B.** Disable auto-summary in RIP and EIGRP.
**C.** Enable loose mode uRPF.
**D.** Change the first statement in access list 100 to permit access.
**Answer: (SHOW ANSWER)**
By redistributing EIGRP into RIP on R1, routes learned via EIGRP will be shared with RIP, allowing R3 to learn the route to Host C's network. This will enable Host B to successfully ping Host C.

**NEW QUESTION: 55**
What does the MP-BGP OPEN message contain?

**A.** MPLS labels and the IP address of the router that receives the message
**B.** the version number and the AS number to which the router belongs
**C.** IP routing information and the AS number to which the router belongs
**D.** NLRI, path attributes, and IP addresses of the sending and receiving routers
**Answer: (SHOW ANSWER)**
The OPEN message contains the BGP version number, ASN of the originating router, Hold Time, BGP Identifier, and other optional parameters that establish the session capabilities.

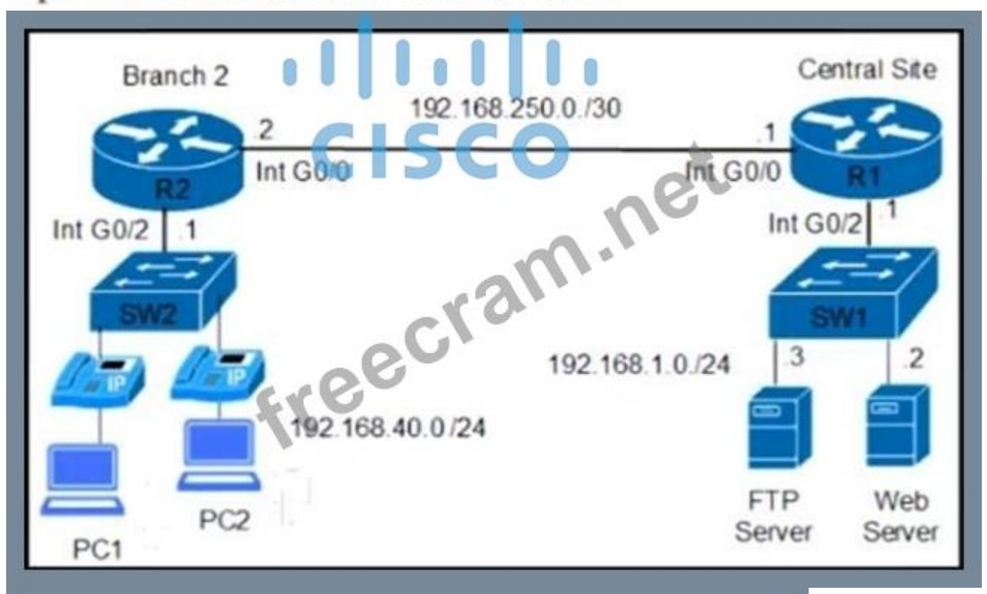
**NEW QUESTION: 56**
Refer to the exhibit. The static route is not present in the routing table of an adjacent OSPF neighbor router. Which action resolves the issue?

```
ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
     match ip addresss prefix-list DMZ-STATIC
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
redistribute static route-map DMZ
!
ip route 10.1.1.0 255.255.255.0 10.20.20.1
```

**A.** Configure the next hop of 10.20.20.1 in the prefix list DMZ-STATIC
**B.** Configure the next-hop interface at the end of the static router for it to get redistributed
**C.** Configure a permit 20 statement to the route map to redistribute the static route
**D.** Configure the subnets keyword in the redistribution command
**Answer: D (LEAVE A REPLY)**
When you include the subnets keyword, the OSPF redistributes the routes, which are subnetted.
The process uses 20 as the default metric. This happens when no metric is specified by the use of the metric-type keyword.

**NEW QUESTION: 57**
Refer to the exhibit. Branch 2 hosts cannot receive dynamic IP addresses. Which action resolves the issue?

```
R2
!
interface GigabitEthernet0/0
 ip address 192.168.250.2 255.255.255.252
 ip helper-address 192.168.250.1
!
interface GigabitEthernet0/2
 ip address 192.168.40.1 255.255.255.0
```




```
R1
!
ip dhcp excluded-address 192.168.40.1 192.168.40.10
!
ip dhcp pool Branch 2
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.1.40
```

**A.** Configure the ip helper command on the Layer 2 switch SW2 interfaces.
**B.** Configure the ip helper command on the Interface GigabltEthernet 0/0 of the DHCP router.
**C.** Configure the ip helper command on the Interface GigabltEthernet 0/2 of the DHCP router.
**D.** Configure the ip helper command on the interface GigabltEthernet 0/2 of the R2 router.

**Answer: (SHOW ANSWER)**

The hosts in Branch 2 on the 192.168.40.0/24 network need a DHCP server to obtain IP addresses. The DHCP server is located on R1, which is in a different subnet. DHCP requests are broadcast messages, and broadcasts do not cross routers by default. To forward these DHCP requests to the DHCP server, the ip helper-address command must be configured on the interface closest to the requesting hosts (in this case, R2's GigabitEthernet 0/2 interface).

This ensures that DHCP requests from Branch 2's subnet are forwarded to the DHCP server on R1.

**NEW QUESTION: 58**

Refer to the exhibit. The Customer Edge router (AS 65500) wants to use AS 100 as the preferred ISP for all external routes.

Customer Edge

route-map SETLP

set local-preference 111

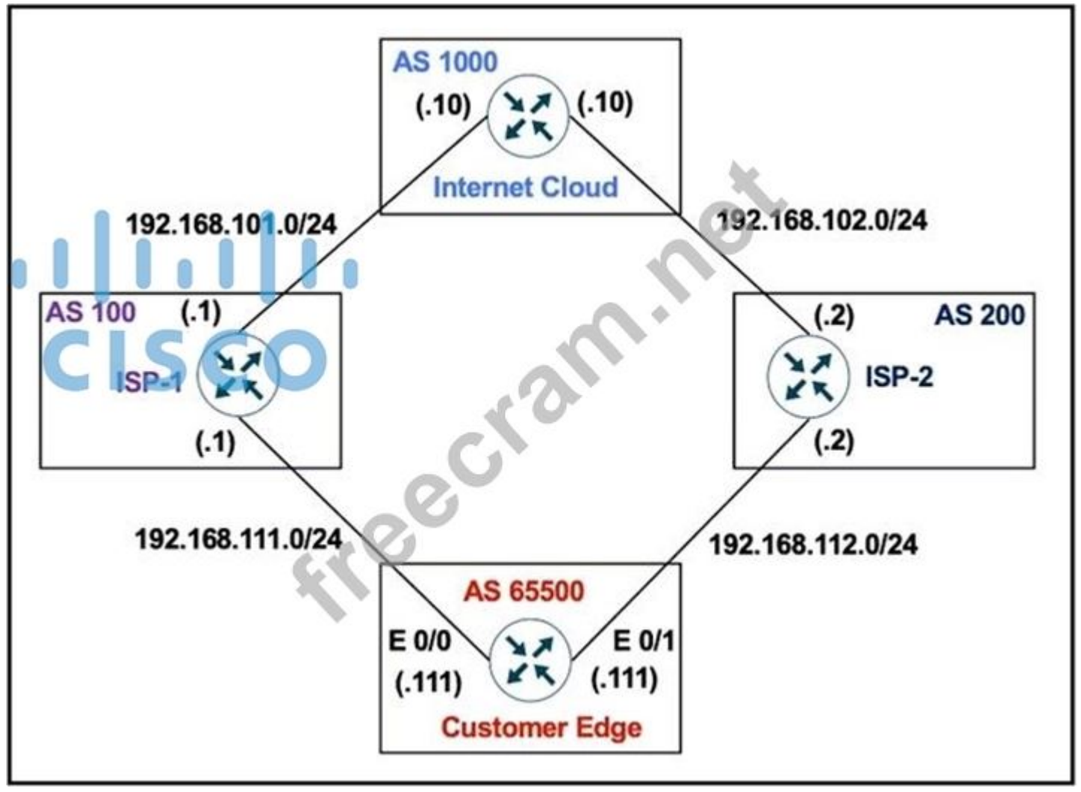
!

router bgp 65500

neighbor 192.168.111.1 remote-as 100

neighbor 192.168.111.1 route-map SETLP out

neighbor 192.168.112.2 remote-as 200




This configuration failed to send routes to AS 100 as the preferred path. Which set of configurations resolves the issue?

**A.** route-map SETLP

set local-preference 111

!

router bgp 65500

neighbor 192.168.111.1 remote-as 100

neighbor 192.168.111.1 route-map SETLP in

**B.** route-map SETPP

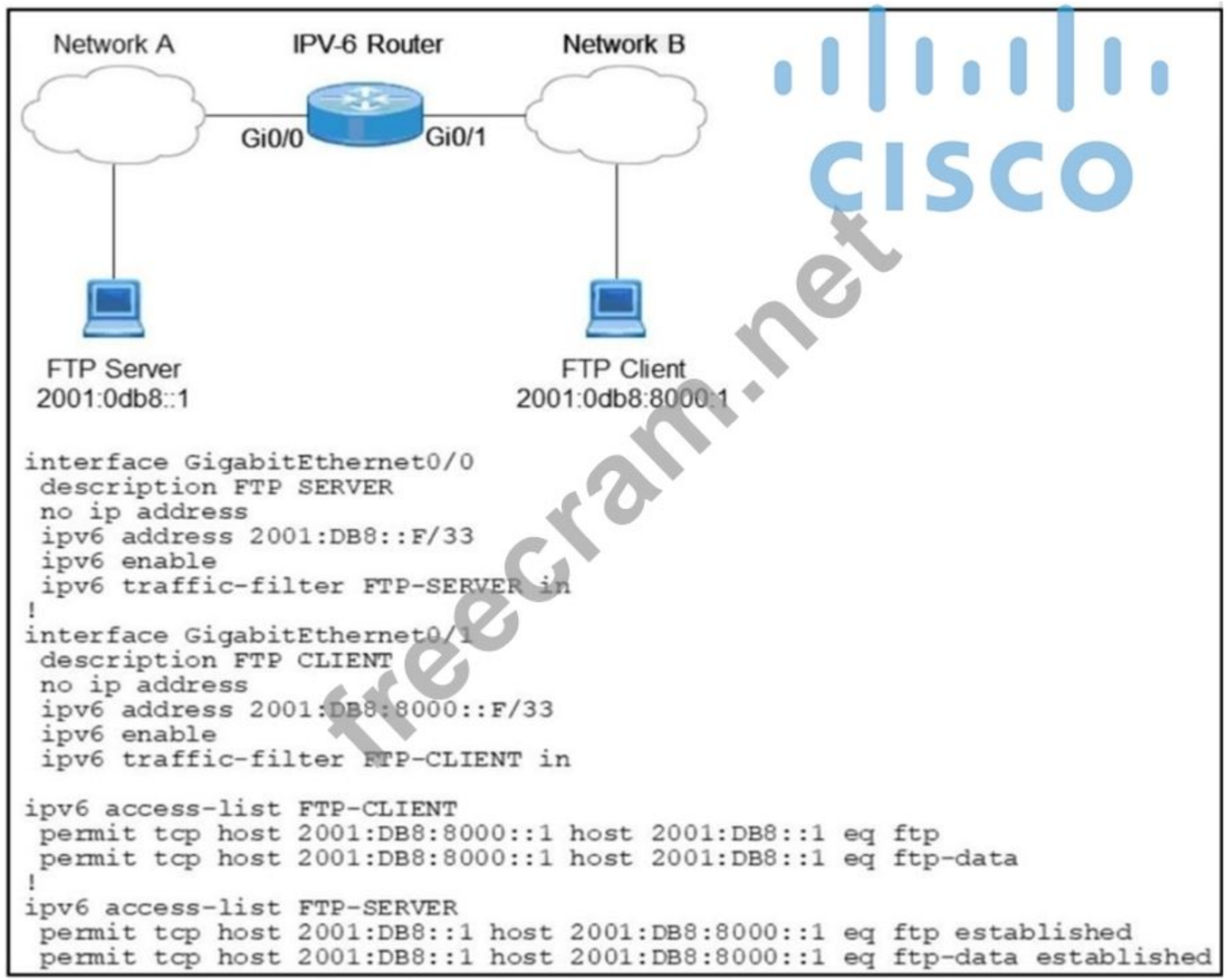
set as-path prepend 100 100

!

router bgp 65500
neighbor 192.168.111.1 remote-as 100
neighbor 192.168.111.1 route-map SETPP in
**C.** route-map SETPP
set as-path prepend 111 111
!
router bgp 65500
neighbor 192.168.111.1 remote-as 100
neighbor 192.168.111.1 route-map SETPP out
**D.** route-map SETLP
set local-preference 111
!
router bgp 65500
neighbor 192.168.111.1 remote-as 100
neighbor 192.168.111.1 route-map SETLP out
**Answer: (SHOW ANSWER)**
In BGP, the local-preference attribute is used to prefer one path over another for outbound traffic.
The local-preference attribute is not sent to external BGP (eBGP) peers; it is an attribute evaluated within the local AS.
The issue in the provided configuration is that the route-map SETLP is applied in the outbound direction, which is ineffective since local-preference does not leave the AS. To resolve the issue, the route-map SETLP should be applied in the inbound direction (route-map SETLP in), allowing the local-preference attribute to influence route selection for traffic leaving AS 65500.

**NEW QUESTION: 59**
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) R1#sh run | s bgp router bgp 65001 no synchronization bgp router-id 10.100.1.50 bgp log-neighbor-changes network 10.1.1.0 mask 255.255.255.252 network 10.1.1.12 mask 255.255.255.252 network 10.100.1.50 mask 255.255.255.255 timers bgp 20 60 neighbor R2 peer-group neighbor R4 peer-group neighbor 10.1.1.2 remote-as 65001 neighbor 10.1.1.2 peer-group R2 neighbor 10.1.1.14 remote-as 65001 neighbor 10.1.1.14 peer-group R4 no auto-summary
**A.** neighbor R2 route-reflector-client
**B.** neighbor 10.1.1.2 route-reflector-client
**C.** neighbor 10.1.1.2 allowas-in
**D.** neighbor R4 route-reflector-client
**E.** neighbor 10.1.1.14 route-reflector-client
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 60**
Refer to the exhibit. When an FTP client attempts to use passive FTP to connect to the FTP server, the file transfers fail Which action resolves the issue?




```
interface GigabitEthernet0/0
 description FTP SERVER
 no ip address
 ipv6 address 2001:DB8::F/33
 ipv6 enable
 ipv6 traffic-filter FTP-SERVER in
!
interface GigabitEthernet0/1
 description FTP CLIENT
 no ip address
 ipv6 address 2001:DB8:8000::F/33
 ipv6 enable
 ipv6 traffic-filter FTP-CLIENT in

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

**A.** Configure active FTP traffic.

**B.** Modify FTP-SERVER access list to remove established at the end.

**C.** Modify traffic filter FTP-SERVER in to the outbound direction.

**D.** Configure to permit TCP ports higher than 1023.

**Answer: (SHOW ANSWER)**

Port numbers above 1023 can be either registered or dynamic (also called private or non- reserved). Registered ports are in the range 1024 to 49151. Dynamic ports are in the range 49152 to 65535. As mentioned, most new port assignments are in the range from 1024 to 49151.

**NEW QUESTION: 61**

Which two features are provided by EIGRP for IPv6? (choose two)

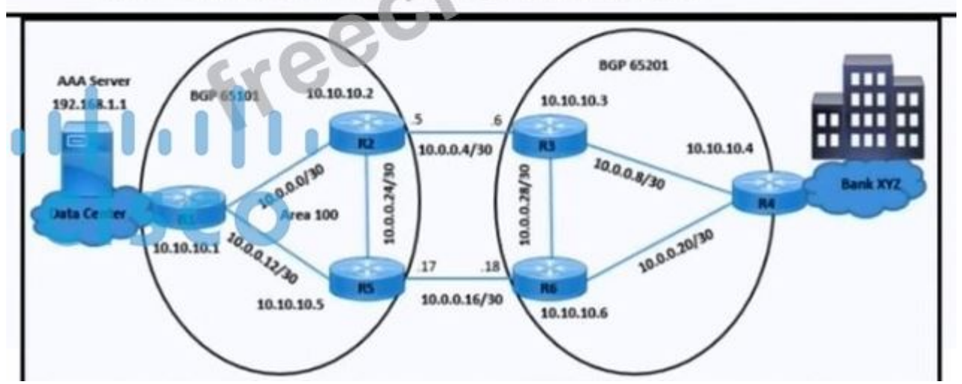
**A.** SPF algorithm

**B.** Area border router
**C.** Backbone areas
**D.** Partial updates
**E.** Scaling
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 62**
Refer to the exhibit. A customer reports that user traffic of bank XYZ to the AAA server is not using the primary path via the R3-R2 link. The network team observes:
- No fiber is cut on links R2 and R3.
- AS101 and AS 201 routers established BGP peering.
Which configuration resolves the issue?

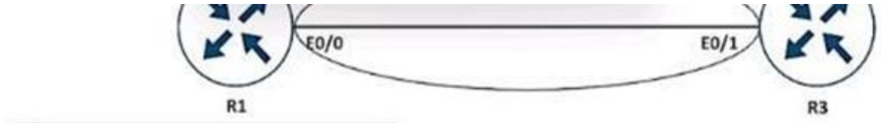
```
R1#show ip bgp 10.10.10.4/32
BGP routing table entry for 10.10.10.4/32, version 21
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Not advertised to any peer
  65201
    10.10.10.5 (metric 2) from 10.10.10.5 (10.10.10.5)
      Origin IGP, metric 0, localpref 100, valid, internal
  65201
    10.10.10.2 (metric 2) from 10.10.10.2 (10.10.10.2)
      Origin IGP, metric 0, localpref 100, valid, internal, best

R4#show ip bgp 192.168.1.1/32
BGP routing table entry for 192.168.1.1/32, version 24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65101
    10.10.10.6 (metric 156160) from 10.10.10.6 (10.10.10.6)
      Origin IGP, metric 0, localpref 100, weight 32769, valid, internal, best
  65101
    10.10.10.3 (metric 2) from 10.10.10.3 (10.10.10.3)
      Origin IGP, metric 0, localpref 100, valid, internal
```




Refer to the exhibit. A customer reports that user traffic of bank XYZ to the AAA server is not using the primary path via the R3-R2 link. The network team observes:

* No fiber is cut on links R2 and R3.
* AS101 and AS 201 routers established BGP peering.
Which configuration resolves the issue?
**A.** R6(config)#router bgp 65201
R6(config-router)#no neighbor 10.10.10.5 weight 32769
**B.** R1(config)#route-map BGP-Path permit 10
R1(config-route-map)# set local-preference 200
R1(config)#router bgp 65101
R1 (config-router)# neighbor 10.10.10.2 route-map BGP-Path out
**C.** R4(config)#router bgp 65201
RA(config-router)#no neighbor 10.10.10.6 weight 32769
**D.** R2(config)#route-map BGP-Path permit 10
R2(config-route-map)# set metric 200
R2(config)#router bgp 65101
R2(config-router)# neighbor 10.10.10.3 route-map BGP-Path out
**Answer: (SHOW ANSWER)**
The issue arises because traffic is not using the primary path between R2 and R3 due to the weight attribute on R6. The weight attribute is a BGP path selection criterion that is locally significant and overrides other metrics. In this case, R6 prefers the route through 10.10.10.6 (via R5) because of the higher weight (32769) set on this neighbor.
To resolve the issue, remove the weight 32769 configuration on R6 for neighbor 10.10.10.5. By doing so, the default weight (0) will be used, allowing the primary path (via R3 and R2) to be selected based on other BGP path attributes, such as Local Preference or AS Path. This change ensures that the desired path (via R3 and R2) is preferred.

**NEW QUESTION: 63**
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?




```
R1
service timestamps debug datetime msec
service timestamps log datetime msec
!
clock timezone EET 2 0
!
end
```

```
R1#show clock
*23:50:13.297 EET Sat Nov 14 2020

R1#
*Nov 14 21:49:59.607: IP: s=10.1.1.1 (local), d=224.0.0.5 (Ethernet0/0), len 80, local feature, Logical MN local(14), rtype 0,
forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Nov 14 21:49:59.607: IP: s=10.1.1.1 (local), d=224.0.0.5 (Ethernet0/0), len 80, sending broad/multicast
*Nov 14 21:49:59.607: IP: s=10.1.1.1 (local), d=224.0.0.5 (Ethernet0/0), len 80, sending full packet
*Nov 14 21:50:00.336: IP: s=10.2.2.4 (Ethernet0/1), d=224.0.0.5, len 80, rcvd 0
*Nov 14 21:50:00.336: IP: s=10.2.2.4 (Ethernet0/1), d=224.0.0.5, len 80, input feature, packet consumed, MCI Check(101),
rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
```



**A.** service timestamps debug datetime msec show-timezone

**B.** service timestamps datebug datetime localtime msec
**C.** service timestamps log datetime locatetime msec
**D.** service timestamps log datetime msec show-timezone
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 64**
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 about not receiving the summary route with the specific loopback address. Which two configurations will fix this issue? (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.** route-map Leak-Route permit 20
**B.** access-list 1 permit 10.1.1.1 0.0.0.252
**C.** route-map Leak-Route permit 10 and match access-list 1
**D.** access-list 1 permit 10.1.1.0 0.0.0.3
**E.** access-list 1 and match under route-map Leak-Route
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 65**
A newly installed 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.** session message
**C.** extended discovery message
**D.** notification message
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 66**
Which of the following OSPF Link State Advertisements (LSA's) were created for IPV6 and do not apply to IPv4 OSPF networks? (Choose two.)
**A.** Link LSA (Type 8)
**B.** Opaque LSA (Type 9)
**C.** Summary LSA (Type 3)
**D.** Router LSA (Type 2)
**E.** Intra-Area Prefix LSA (Type 9)
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 67**
Drag and Drop Question
Drag and drop the actions from the left into the order on the right to configure a policy to avoid following packet forwarding based on the normal routing path.

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

**Answer:**

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

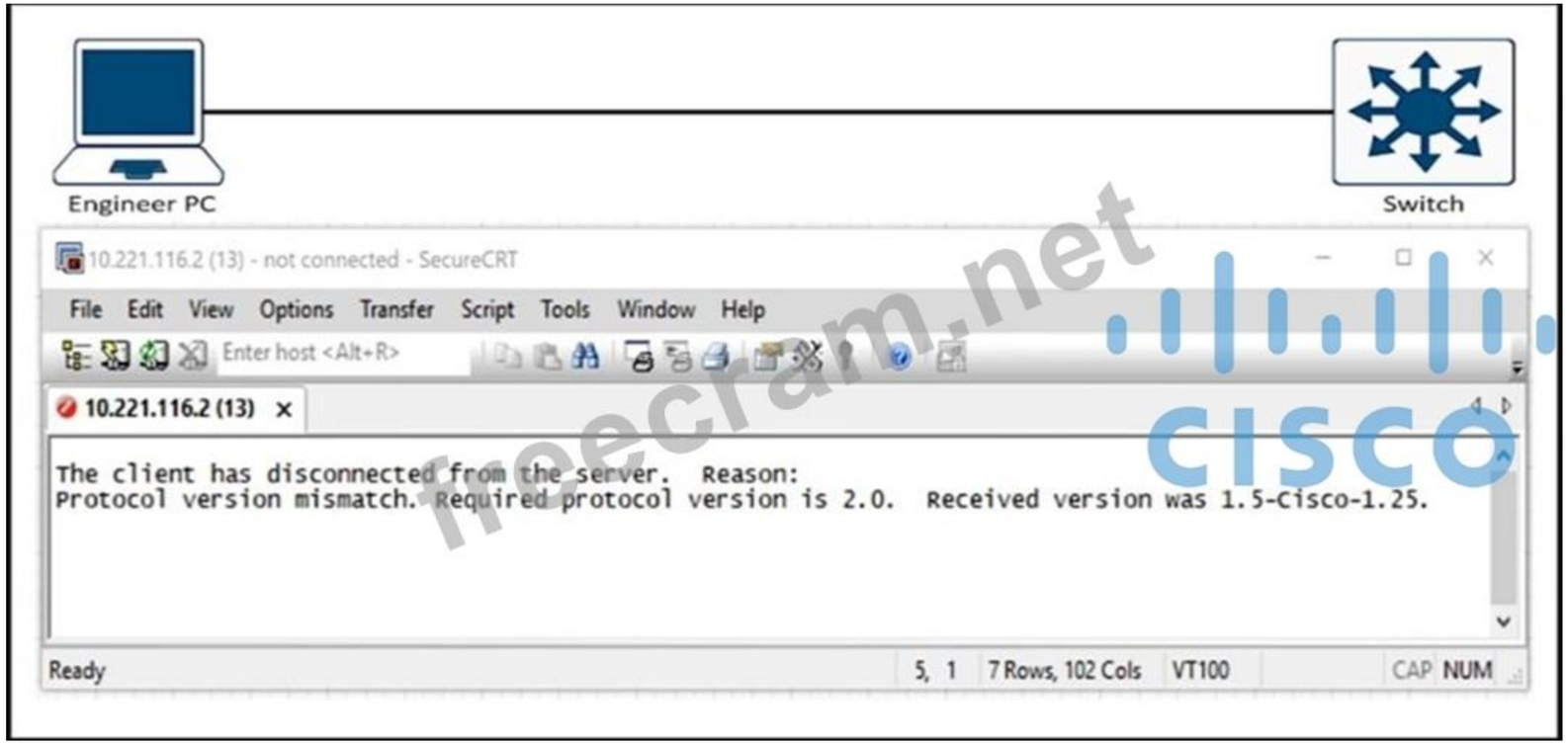
Explanation:
https://community.cisco.com/t5/networking-documents/how-to-configure-pbr/ta-p/3122774

**NEW QUESTION: 68**
What is the output of the following command:
show ip vrf
**A.** Shows default RD values
**B.** Displays IP routing table information associated with a VRF
**C.** Shows routing protocol information associated with a VRF.
**D.** Displays the ARP table (static and dynamic entries) in the specified VRF
**Answer: (SHOW ANSWER)**
An example of the "show ip vrf" is shown below:

```
Router#show ip vrf
 Name                              Default RD          Interfaces
 SiteA2                            103:30              Serial1/0.20
 SiteB                             103:11              Serial1/0.100
 SiteX                             103:20              Ethernet0/0
```

**NEW QUESTION: 69**
Refer to the exhibit. An engineer tried to access the Cisco WS-C6513 core switch but failed.

Which protocol resolves the issue?




**A.** SNMP version 2
**B.** HTTP version 2
**C.** SCP version 2
**D.** SSH version 2
**Answer: (SHOW ANSWER)**
The error shows a protocol version mismatch where the device expects version 2.0 but received version 1.5, which corresponds to SSHv1. The connection fails because the switch requires SSH version 2, so using SSHv2 resolves the issue.

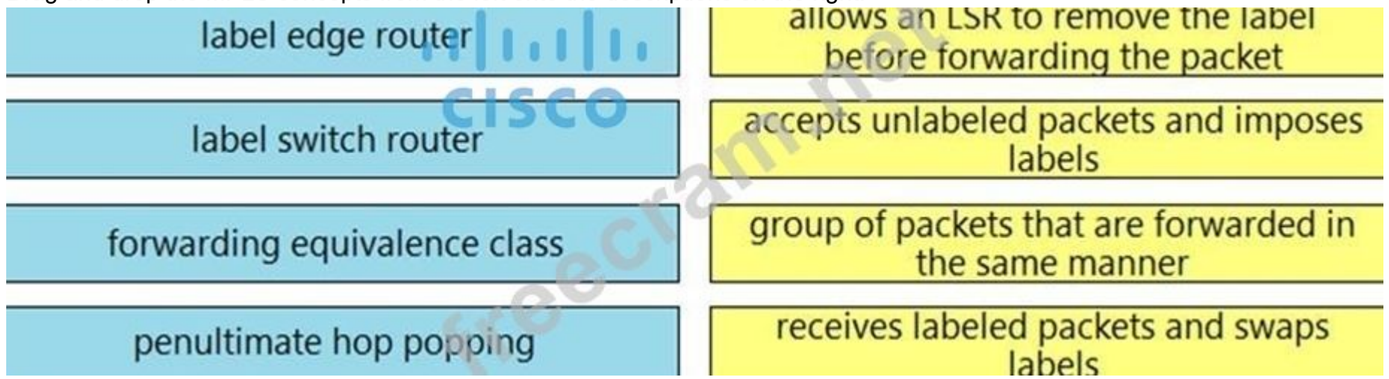
**NEW QUESTION: 70**
Refer to the exhibit. Which option describes why the EIGRP neighbors of this router are not learning routes that are received from OSPF?

```
router eigrp 1
redistribute ospf 100
network 10.10.10.0 0.0.0.255
auto-summary
!
router ospf 100
network 172.16.0.0. 0.0.255.255 area 100
redistribute eigrp 1
```

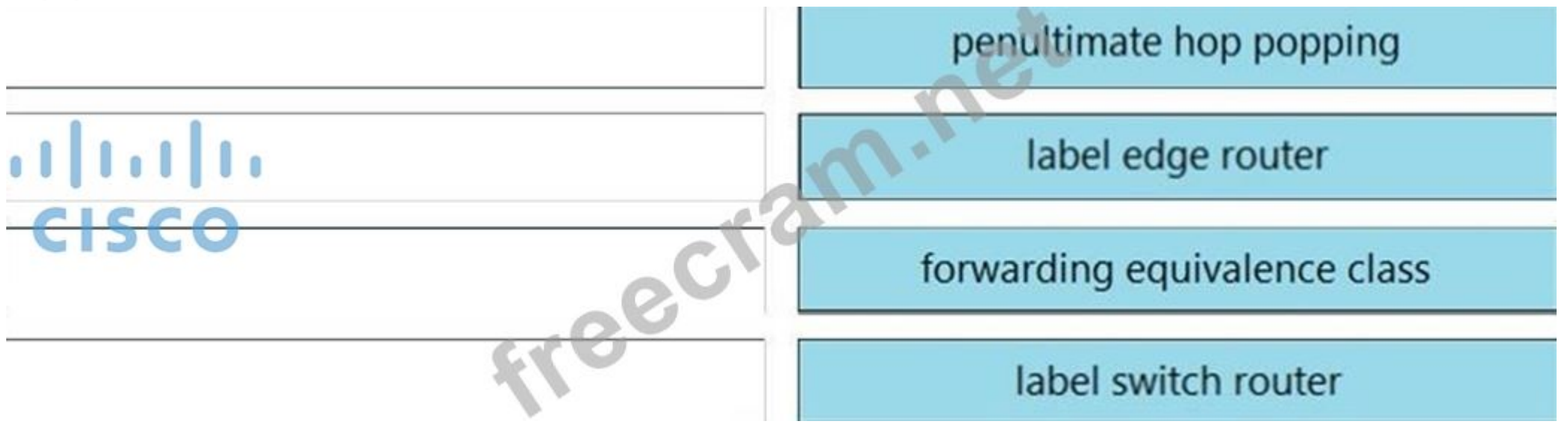
**A.** The subnet defined in OSPF is not part of area 0
**B.** Default metrics are not configured under EIGRP

**C.** There is no overlap in the subnets advertised
**D.** The routing protocols do not have the same AS number
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 71**
Drag and Drop Question
Drag and drop the MPLS concepts from the left onto the descriptions on the right.




**Answer:**




Explanation:
A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERspush an MPLS label onto an incoming packet and pop it off an outgoing packet.
A forwarding equivalence class (FEC) is a term.

**NEW QUESTION: 72**
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 reply and advertisements from (rouge) DHCPv6 servers.

**Answer: (SHOW ANSWER)**
The DHCPv6 Guard feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers (-> Answer D is not correct) and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked (-> Answer C is not correct) Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6f-xe-16-book/ip6-dhcpv6-guard.html

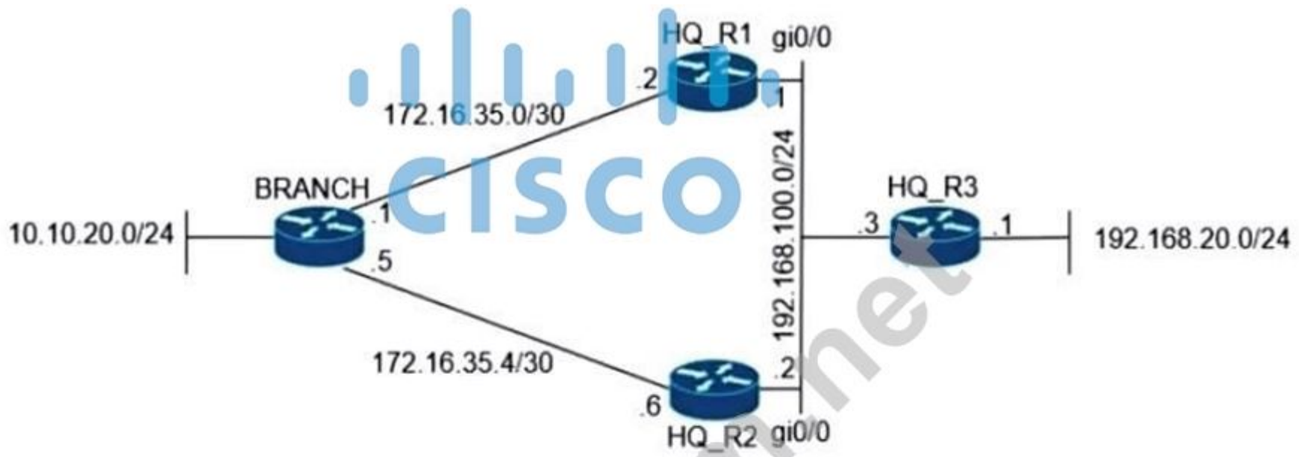
**NEW QUESTION: 73**
Which feature of the Cisco DNA Center allows you to run diagnostic CLI commands to the devices that are managed by DNA Center for troubleshooting purposes?
**A.** DNA Advantage
**B.** DNA Spaces
**C.** Intelligent Capture
**D.** Command Runner
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 74**
What are two MPLS label characteristics? (Choose two.)
**A.** The label edge router swaps labels on the received packets.
**B.** Labels are imposed in packets after the Layer 3 header.
**C.** LDP uses TCP for reliable delivery of information.
**D.** An MPLS label is a short identifier that identifies a forwarding equivalence class.
**E.** A maximum of two labels can be imposed on an MPLS packet.
**Answer: (SHOW ANSWER)**
A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERs push an MPLS label onto an incoming packet and pop it off an outgoing packet.
MPLS labels are added between the Layer 2 and the Layer 3 header in the packets (-> Therefore MPLS labels are added before Layer 3 header).
There are no limit on the number of labels in a stack.
A label is a short, four-byte, fixed-length, locally-significant identifier which is used in order to identify a Forwarding Equivalence Class (FEC). The label which is put on a particular packet represents the FEC to which that packet is assigned.
LDP uses TCP as a reliable transport for sessions. Each TCP connection has only one LDP session.
Reference: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching- mpls/mpls/4649-mpls-faq-4649.html

**NEW QUESTION: 75**
A customer requested a GRE tunnel through the provider network between two customer sites using loopback to hide internal networks.
Which configuration on R2 establishes the tunnel with R1?
**A.** R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 192.168.20.1
R2(config-if)# tunnel destination 192.168.10.1
**B.** R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0

R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 10.10.2.2
R2(config-if)# tunnel destination 10.10.1.1
**C.** R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1500
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 192.168.20.1
R2(config-if)# tunnel destination 10.10.1.1
**D.** R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1500
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 10.10.2.2
R2(config-if)# tunnel destination 10.10.1.1
**Answer: (SHOW ANSWER)**
The Transmission Control Protocol (TCP) Maximum Segment Size (MSS) Adjustment feature enables the configuration of the maximum segment size for transient packets that traverse a router, specifically TCP segments with the SYN bit set. Use the ip tcp adjust-mss command in interface configuration mode to specify the MSS value on the intermediate router of the SYN packets to avoid truncation.

**NEW QUESTION: 76**
Refer to the exhibit. An engineer has successfully set up a floating static route from the BRANCH router to the HQ network using HQ_R1 as the primary default gateway.
When the g0/0 goes down on HQ_R1, the branch network cannot reach the HQ network
192.168.20.0/24.
Which set of configurations resolves the issue?




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

**A.** HQ_R3(config)# ip sla responder
HQ_R3(config)# ip sla responder icmp-echo 172.16.35.1
**B.** BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 192.168.100.2
**C.** HQ R3(config)# ip sla responder
HQ R3(config)# ip sla responder icmp-echo 172.16.35.5
**D.** BRANCH(config)# ip sla 1
BRANCH(config-ip-sta)# icmp-echo 192.168.100.1
**Answer: (SHOW ANSWER)**
By monitoring the ip address on the other side of the router you can make sure that if it goes down, the failover will occur. The way it was configured if g0/0 went down, then the SLA monitor would not fail and no failover would occur.

**NEW QUESTION: 77**
Refer to the exhibit. Which action resolves the failed authentication attempt to the router?

**Configuration Output:**

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


password 7 k0AyUudDrfOgO4s
authorization exec VTY_AUTH
login authentication VTY_AUTH

!
```

**Debug Output**

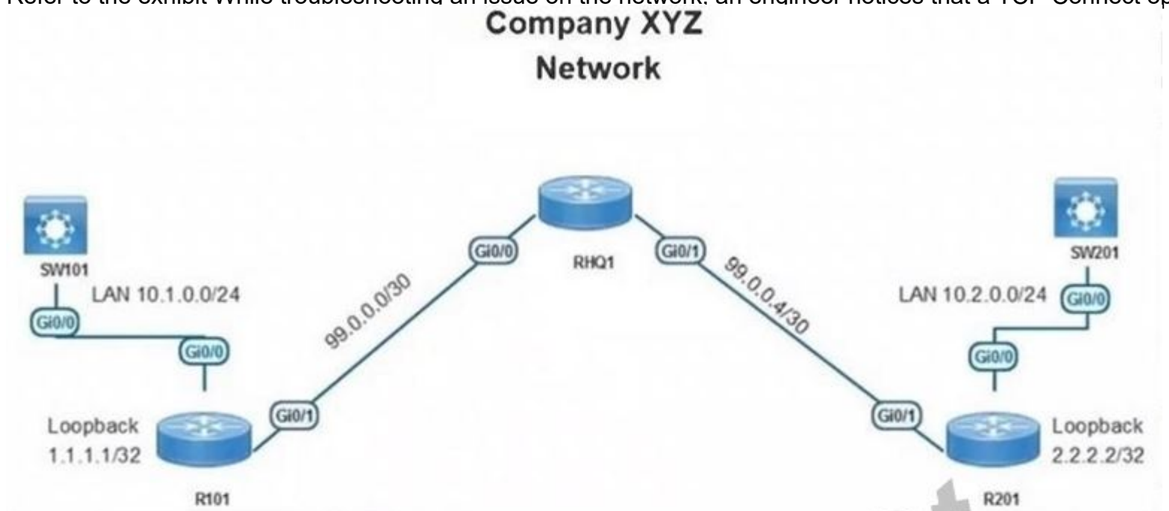
```
AAA/AUTHEN/LOGIN (000004B6): Pick method list 'default'
AAA/AUTHOR (0x4B6): Pick method list 'VTY_AUTH'
AAA/AUTHOR/EXEC(000004B6): Authorization FAILED
```

**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: 78**
Which IPv6 first hop security feature controls the traffic necessary for proper discovery of neighbor device operation and performance?

**A.** ND Multicast Suppression
**B.** IPv6 Snooping
**C.** RA Throttling
**D.** Source or Destination Guard
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 79**
Refer to the exhibit While troubleshooting an issue on the network, an engineer notices that a TCP Connect operation failed on port 3000 between R101 and R201. Which command must be configured on R201 to respond




```
R101#sh run | section sla
ip sla 1
   tcp-connect 2.2.2.2 3000 source-ip 1.1.1.1
   threshold 1000
   timeout 1000
   frequency 10
ip sla schedule 1 life forever start-time now
ip sla 2
   icmp-jitter 2.2.2.2 source-ip 1.1.1.1 num-packets 100 interval 10
   threshold 1000
   timeout 1000
   frequency 10
ip sla schedule 2 life forever start-time now
R101#sh ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID   Type        Destination   Stats (ms)  Return Code      Last Run
---------------------------------------------------------------------
*1   tcp-connect 2.2.2.2       -           No connection    33 seconds ago
*2   icmp-jitter 2.2.2.2       RTT=4       OK               3 seconds ago
```

**A.** ip sla responder tcp-connect ipaddress 2.2.2.2 port 3001
**B.** ip sla responder udp-echo ipaddress 1.1.1.1 port 1967
**C.** ip sla responder tcp-connect ipaddress 1.1.1.1 port 3000
**D.** ip sla responder
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 80**
Refer to the exhibit. A network engineer notices that the configured track option is down. Which configuration resolves the issue?

```
R1#sh track brief
Track Type        Instance                Parameter       State Last Change

1     ip sla      10                      reachability    Down  00:03:52


R1#show ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 10
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source interface: 10.10.10.10/GigabitEthernet0/0
<->
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
```

**A.** ip sla schedule 10 start-time now
**B.** ip sla schedule 10 start-time pending life forever
**C.** ip sla schedule 10
no threshold
**D.** ip sla schedule 10
no timeout
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 81**
What is the role of a route distinguisher via a VRF-Lite setup implementation?
**A.** It extends the IP address to identify which VFP instance it belongs to.

**B.** It manages the import and export of routes between two or more VRF instances

**C.** It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities

**D.** It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities

**Answer: (SHOW ANSWER)**

In VRF-Lite, Route distinguisher (RD) identifies the customer routing table and "allows customers to be assigned overlapping addresses". The below example shows overlapping IP addresses configured on two interfaces which belong to two different VPNs:

Router(config)#ip vrf VRF_BLUE

Router(config-vrf)# rd 100:1

Router(config-vrf)# exit

Router(config)#ip vrf VRF_GREEN

Router(config-vrf)# rd 100:2

Router(config-vrf)# exit

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip vrf forwarding VRF_BLUE

Router(config-if)# ip address 10.0.0.1 255.0.0.0

Router(config-vrf)# exit

Router(config)# interface GigabitEthernet0/2

Router(config-if)# ip vrf forwarding VRF_GREEN

Router(config-if)# ip address 10.0.0.1 255.0.0.0

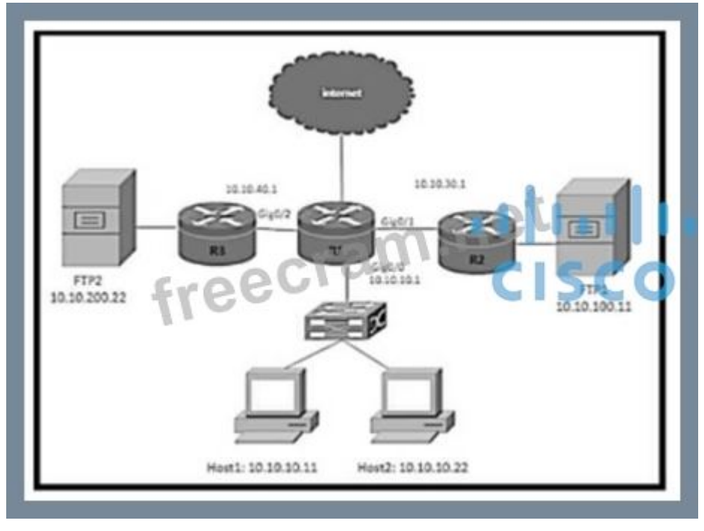
In this example, the RD will be added to the beginning of the IP address. For example with VRF_BLUE (rd 100:1), an IP address will be seen like this: 100:1:10.0.0.1/8 so that it is unique in the routing table.

**NEW QUESTION: 82**

Refer to the exhibit. The R1 routing table has the prefixes for the FTP1 and FTP2 file servers. A network engineer must configure the R1 with these requirements:

- Host1 must use the FTP1 fileserver.
- Host2 must use the FTP2 fileserver.

Which configuration meets the requirement on R1?



A.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.40.1
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.30.1
!
ip local policy route-map PBR_FTP
```

B.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
ip local policy route-map PBR_FTP
```

C.

```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
 set ip next-hop 10.10.40.1
!
interface GigabitEthernet 0/0
 ip policy route-map PBR_FTP
```

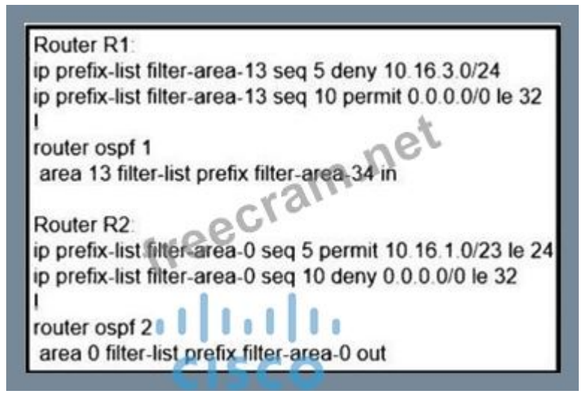

**D.**

**Answer: (SHOW ANSWER)**

Chosen configuration applies the correct source-destination matching for each host and applies the policy-based routing (PBR) on the appropriate interface, ensuring that Host1's traffic reaches FTP1 and Host2's traffic reaches FTP2.

**NEW QUESTION: 83**

Refer to the exhibit. R1 should receive 10.16.2.0/24 from R2. Which action resolves the issue?




**A.** Modify prefix-list seq 5 on R2 to permit 10.16.0.0/22.

**B.** Add prefix-list seq 1 on R1 to permit 10.16.0.0/22.

**C.** Add prefix-list seq 1 on R1 to permit 10.16.2.0/24.

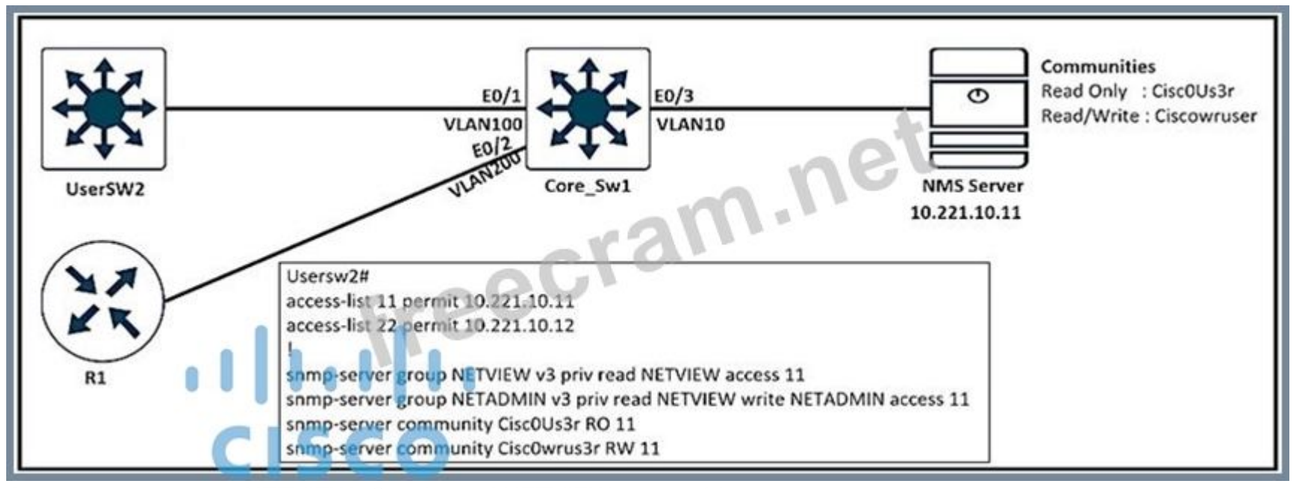
**D.** Modify prefix-list seq 5 on R2 to permit 10.16.0.0/23.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 84**

Refer to the exhibit. An engineer configured SNMP community on UserSW2 switch, but the SNMP server cannot upload modified configurations to the switch.

Which configuration resolves this issue?




**A.** snmp-server group NETVIEW v2c priv read NETVIEW access 11

**B.** snmp-server community CiscOUs3r RW 11

**C.** snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22

**D.** snmp-server community Ciscowruser RW 11

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 85**

Refer to the exhibit. An engineer implements uRPF to increase security and stop incoming spoofed IP packets. Same asymmetrically routed packets are also blocked after the configuration.

Which command resolves the issue?

```
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 -1 Slot unit 3 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
```

**A.** ip verify unicast reverse-path
**B.** ip verify unicast source reachable-via any
**C.** ip verify unicast reverse-path any
**D.** ip verify unicast source reachable-via rx
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 86**
Refer to the exhibit. An administrator must configure the router with OSPF for IPv4 and IPv6 networks under a single process. The OSPF adjacencies are not established and did not meet the requirement. Which action resolves the issue?

```
router ospfv3 1
router-id 10.1.1.1
address-family ipv4 unicast
passive-interface Loopback0
exit-address-family
address-family ipv6 unicast
passive-interface Loopback0
exit-address-family
interface Loopback0
ip address 10.1.1.1 255.255.255.255
ipv6 address 2001:DB8::1/64
ospfv3 10 ipv4 area 10
ospfv3 10 ipv6 area 0
interface GigabitEthernet2
ip address 10.10.10.1 255.255.255.0
ipv6 enable
ospfv3 10 ipv4 area 10
ospfv3 10 ipv6 area 0
```

**A.** Replace OSPF process 10 on the interface with OSPF process 1, and configure an additional router ID with IPv6 address.
**B.** Replace OSPF process 10 on the interface with OSPF process 1, for the VPv6 addressma nd remove process route ID with IPv6 address.
**C.** Replace OSPF process 10 on the interface with OSPF process 1, and remove process 10 from the global configuration.
**D.** Replace OSPF process 10 on the interface with OSPF process 1 for the IPv4 address, and remove process 10 from the global configuration.
**Answer: (SHOW ANSWER)**
The router is configured to use OSPFv3 process 1 globally, but the interfaces are assigned to process 10 for both IPv4 and IPv6. OSPFv3 must use the same process on the interfaces and in the global configuration for adjacencies to form under a single process. Changing the interface configuration to process 1 for both address families resolves the issue.

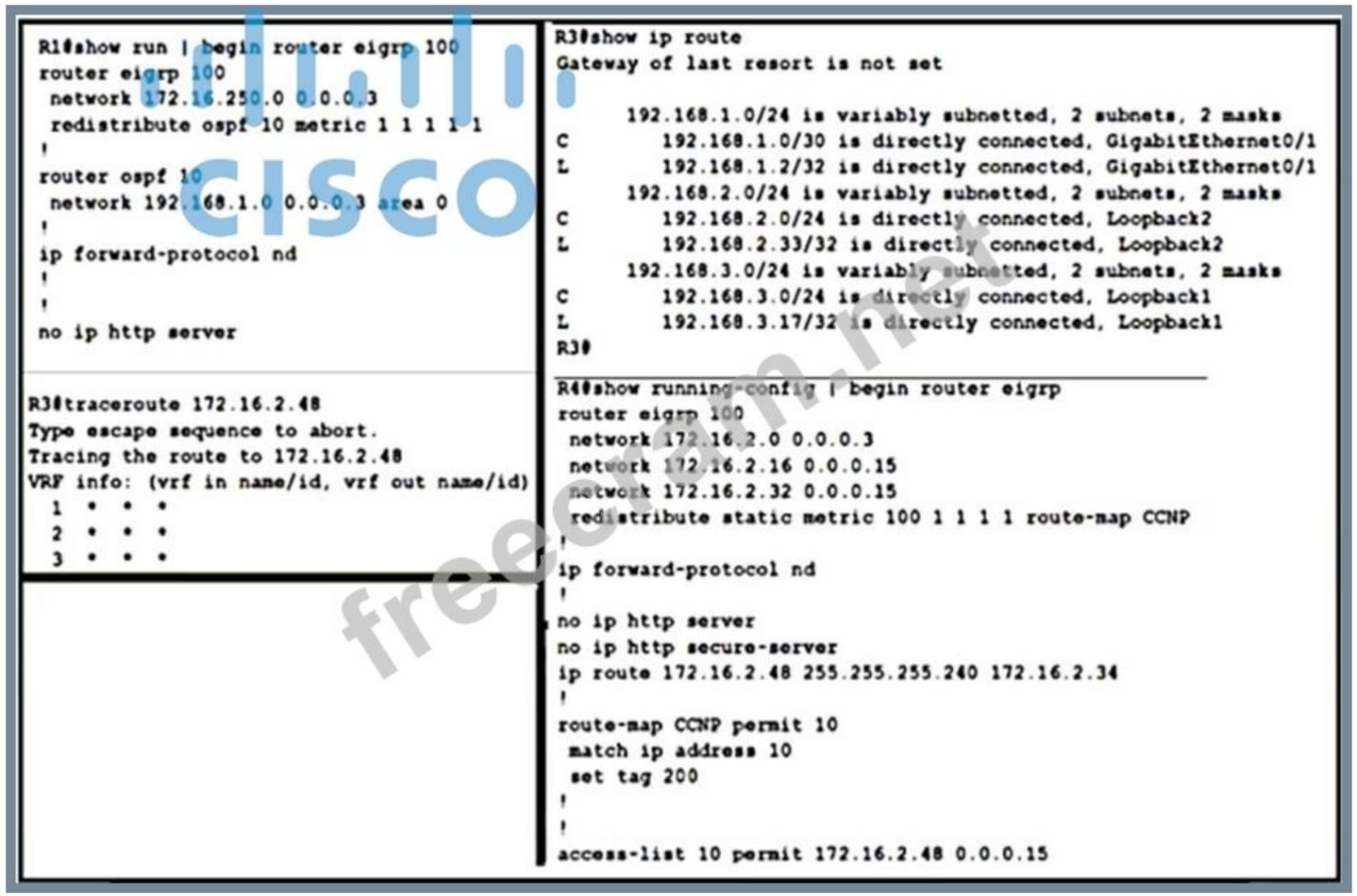
**NEW QUESTION: 87**
Refer to the exhibit. An engineer is troubleshooting BGP on a device but discovers that the clock on the device does not correspond to the time stamp of the log entries.
Which action ensures consistency between the two times?

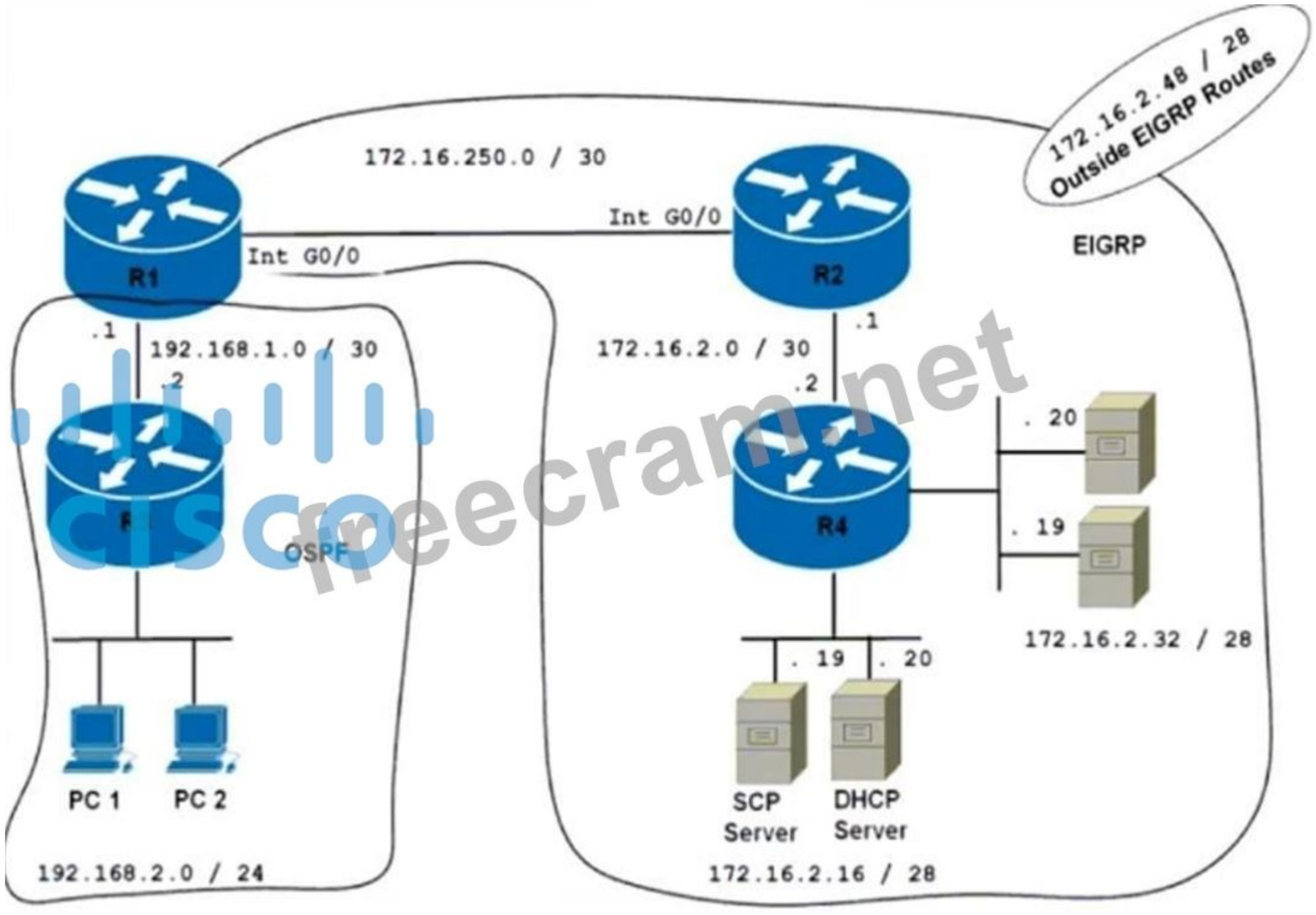
```
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Down User reset
* Jun 28 14:41:57: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.2.2 IPv4 Unicast
topology base removed from session  User reset
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Up
R1#show clock
*15:42:00.506 CET Fri Jun 28 2019
```

**A.** Configure the logging clock synchronize command in global configuration mode
**B.** Configure the service timestamps log uptime command in global configuration mode

**C.** Configure the service timestamps log datetime localtime command in global configuration mode
**D.** Make sure that the clock on the device is synchronized with an NTP server
**Answer: (SHOW ANSWER)**
Even we had a synchronized clock but it may show different timezone so we should set the
"localtime" keyword (which uses local time zone for timestamps) so that the time of logging messages is matched with our clock.
https://community.cisco.com/t5/networking-documents/router-log-timestamp-entries-are-different- from-the-system-clock/ta-p/3132258

**NEW QUESTION: 88**
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 the OSPF domain?








**A.** R1(config)#route-map CCNP permit 10
R1(config-route-map)#match route-type internal
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 100 subnets route-map CCNP
**B.** R1(config)#route-map CCNP deny 10
R1(conflg-route-map)#match tag 200
R1(config)#route-map CCNP permit 10
R1(config)#router ospf 10
R1(conflg-router)#redistrlbute eigrp 100 subnets route-map CCNP
**C.** R1(config)#route-map CCNP permit 10

R1(config-route-map)#match route-type level-2
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 100 subnets route-map CCNP
**D.** R1(config)#route-map CCNP permit 10
R1(config-route-map)#match tag 200
R1(conflg-route-map)#exit
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 100 subnets route-map CCNP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 89**
Refer to exhibit. A network engineer is facing issues between OSPF neighbors changing states frequently. The engineer enabled an ACL for CoPP and applied it at the control plane interface but got unexpected results.
Which action resolves the issue?


**A.** Apply ACL on OSPF physical interface in the outward direction.
**B.** Add one more ACL line to permit 224.0.0.6 in the inward direction.
**C.** Apply ACL on OSPF physical interface in the inward direction.
**D.** Remove the log and log-input keywords from ACL.
**Answer: (SHOW ANSWER)**
The logand log-inputkeywords cause the router to generate a system log message for every matched packet, which adds processing overhead. When used in a Control Plane Policing (CoPP) ACL that matches frequent OSPF packets (such as Hello packets to 224.0.0.5 and
224.0.0.6), this logging can overwhelm the CPU, causing OSPF neighbor adjacencies to flap.
Removing logand log-inputensures efficient packet processing and resolves the OSPF instability.

**NEW QUESTION: 90**
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.** BGPIPv4
**B.** IS-IS
**C.** MP-BGP
**D.** OSPF
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 91**

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.

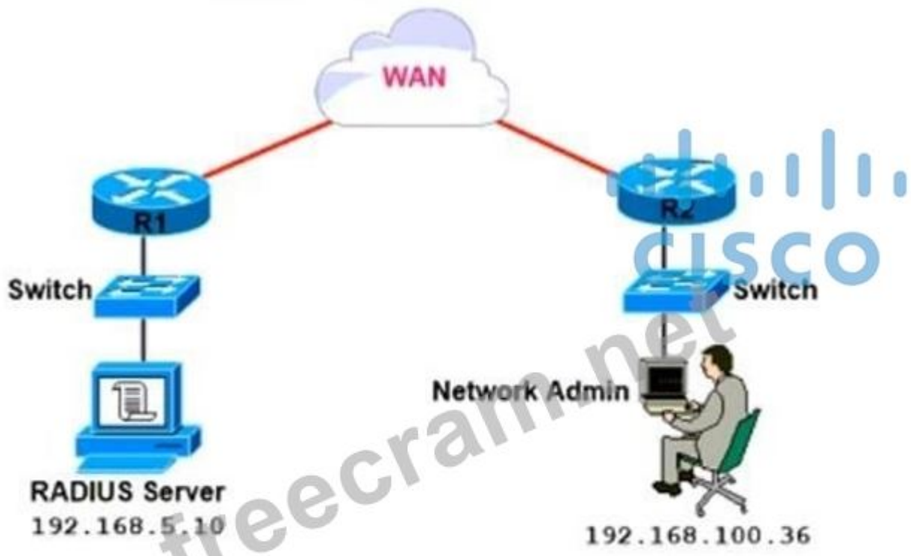
Reference:

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: 92**

Refer to the exhibit. A network administrator is troubleshooting an authentication failure issue during login into R2 using a RADIUS server user account. The network administrator can ping the RADIUS server, but the user

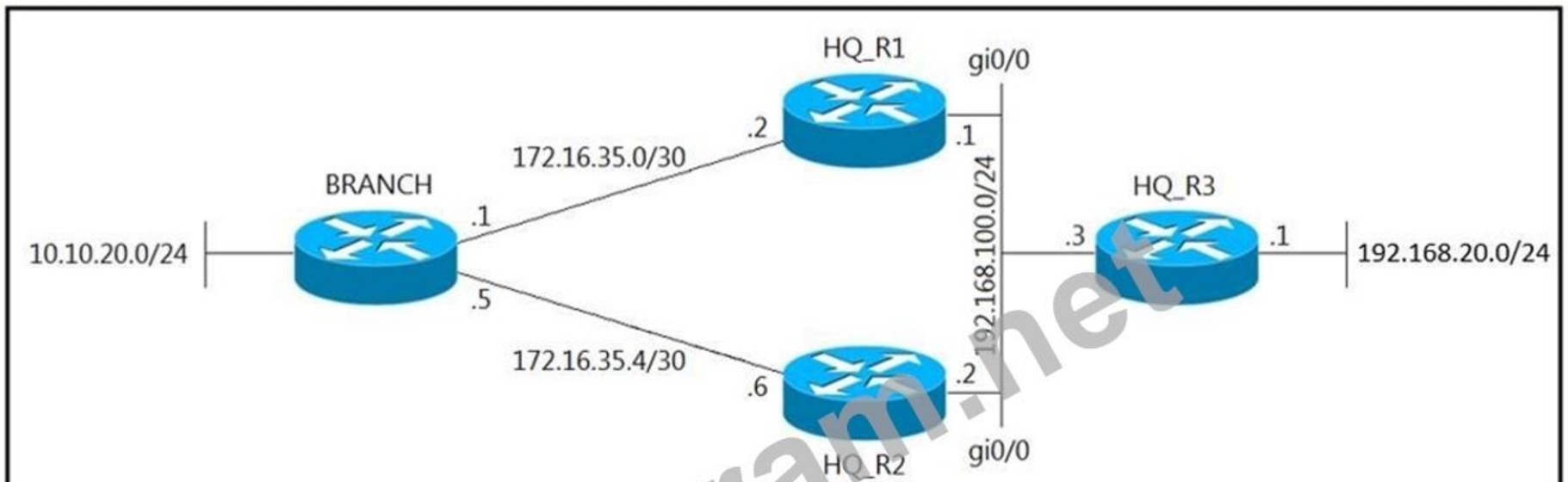





```
R2#
username admin privilege 15 secret 5 $1$qLGb$VQ6BdqCE
aaa new-model
aaa authentication login default group radius group
tacacs+ local
!
radius-server host 192.168.5.10
radius-server key 0 P!cX54$VgQ
```

**A.** Enable AAA authorization to allow SSH connections.
**B.** Configure the username in RADIUS server database.
**C.** Remove "local" from the aaa authentication command.
**D.** Modify the aaa command to replace TACACS+ with RADIUS.
**Answer: (SHOW ANSWER)**
The configuration on R2 specifies that user authentication is done using RADIUS first, then TACACS+, and finally local as a fallback. The RADIUS server is reachable (ping succeeds), and the AAA authentication method is correct.
If the user credentials do not exist in the RADIUS server's user database, authentication will fail, and unless TACACS+ or local fallback is reachable and valid, access will be denied. Adding the appropriate user account (with correct credentials) on the RADIUS server resolves the SSH login issue.

**NEW QUESTION: 93**
Refer to Exhibit. Traffic from the branch network should route through HQ R1 unless the path is unavailable.




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

An engineer tests this functionality by shutting down interface on the BRANCH router toward HQ_R1 router but 192.168.20.0/24 is no longer reachable from the branch router.

Which set of configurations resolves the issue?

**A.** HQ_R2(config)# ip sla responder

HQ_R2(config)# ip sla responder icmp-echo 172.16.35.5

**B.** BRANCH(config)# ip sla 1

BRANCH(config-ip-sla)# icmp-echo 172.16.35.1

**C.** HQ_R1(config)# ip sla responder

HQ_R1(config)# ip sla responder icmp-echo 172.16.35.2

**D.** BRANCH(config)# ip sla 1

BRANCH(config-ip-sla)#icmp-echo 172.16.35.2

**Answer: (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: 94**

What is the use of IPv6 snooping?

**A.** captures IPv6 routing protocol packets to analyze

**B.** requires an external IPv6 packet analyzer

**C.** required for the operation of IPv6 RA Guard

**D.** captures any type of user traffic to create a binding table

**Answer: (SHOW ANSWER)**

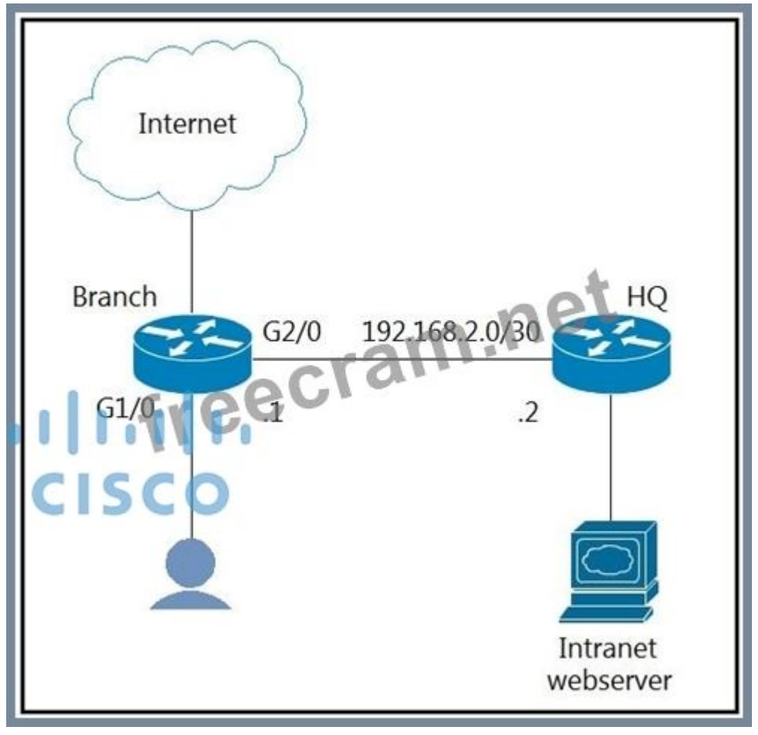
IPv6 snooping captures the IPv6 traffic and helps in populating the binding table. It gathers addresses in control messages such as Neighbor Discovery Protocol (NDP) or Dynamic Host Configuration Protocol (DHCP) packets. Depending on the security level, it blocks unwanted messages such as Router Advertisements (RA) or DHCP replies. This feature is a pre-requisite to the remaining security features mentioned here.

https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_boo k/IPv6_Security.html

**NEW QUESTION: 95**

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.

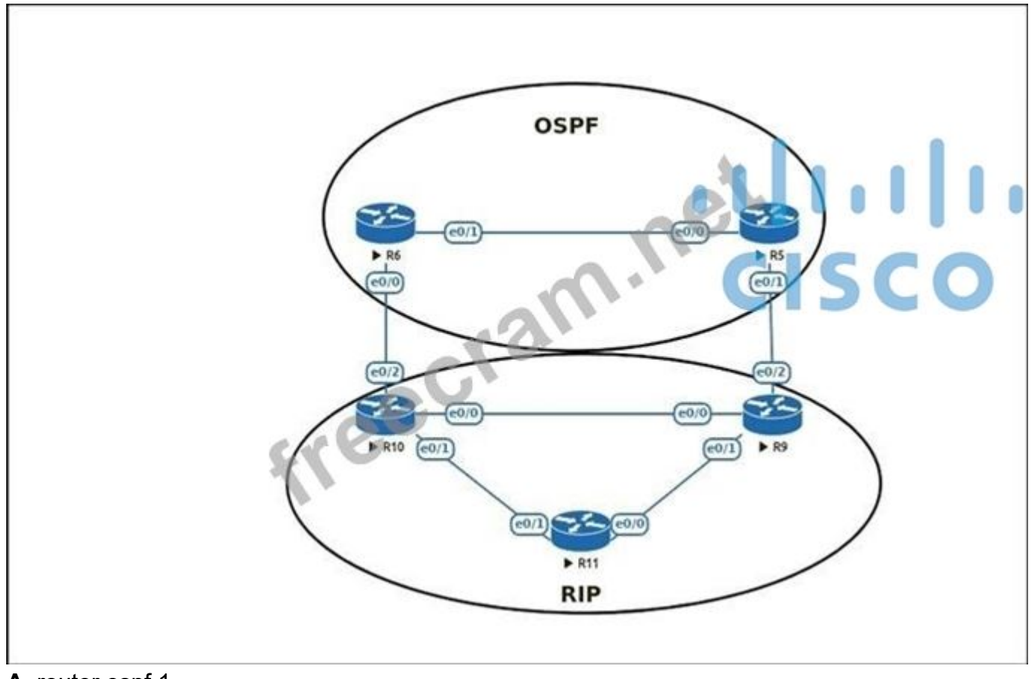
Which configuration on the branch router makes the intranet website (TCP port 80) available to the branch office users?



**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.** access-list 101 permit tcp any any eq 80
access-list 102 permit tcp any host intranet-webserver-ip
!
route-map pbr permit 10
match ip address 101 102
set ip next-hop 192.168.2.2
!
interface G1/0
ip policy route-map pbr
**C.** access-list 101 permit tcp any any eq 80
access-list 102 permit tcp any host intranet-webserver-ip
!
route-map pbr permit 10
match ip address 101
set ip next-hop 192.168.2.2
route-map pbr permit 20
match ip address 102
set ip next-hop 192.168.2.2
!
interface G2/0
ip policy route-map pbr
**D.** access-list 100 permit tcp host intranet-webserver-ip eq 80 any
!
route-map pbr permit 10
match ip address 100
set ip next-hop 192.168.2.2
!
interface G1/0
ip policy route-map pbr
**Answer: (SHOW ANSWER)**
Must include both ACLs on the match statement and applied to the incoming interface.

**NEW QUESTION: 96**

Refer to the exhibit. An engineer must configure OSPF with R9 and R10 and configure redistribution between OSPF and RIP, causing a routing loop. Which configuration on R9 and R10 meets this objective?



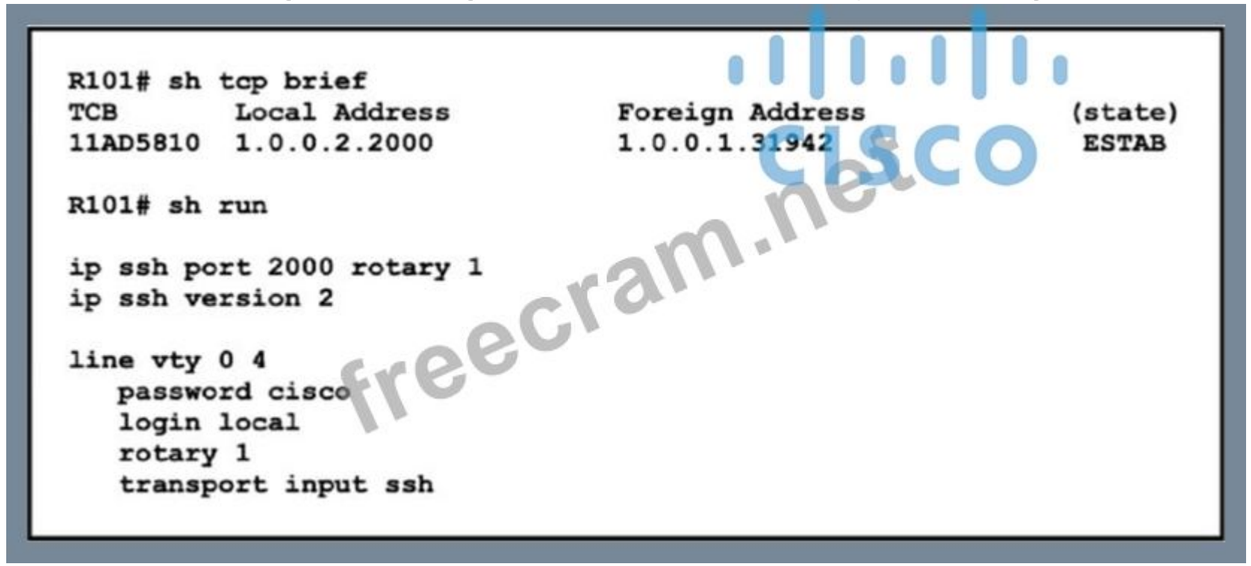

**A.** router ospf 1
redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10
match tag 20
route-map deny_tag20 deny 20
!
router ospf 1
distribute-list route-map deny_tag20 in

**B.** router ospf 1
redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10
match tag 20
route-map deny_tag20 permit 20
!
router rip 1
distribute-list route-map deny _tag20 in

**C.** router ospf 1
redistribute rip subnets tag 20
!
route-map deny_tag20 deny 10

match tag 20
route-map deny_tag20 permit 20
!
router ospf 1
distribute-list route-map deny_tag20 in
**D.** router ospf 1
redistribute rip subnets tag 20
!
route-map deny_tag20 permit 10
match tag 20
route-map deny_tag20 permit 20
!
router ospf 1
distribute-list route-map deny_tag20 in
**Answer: (SHOW ANSWER)**

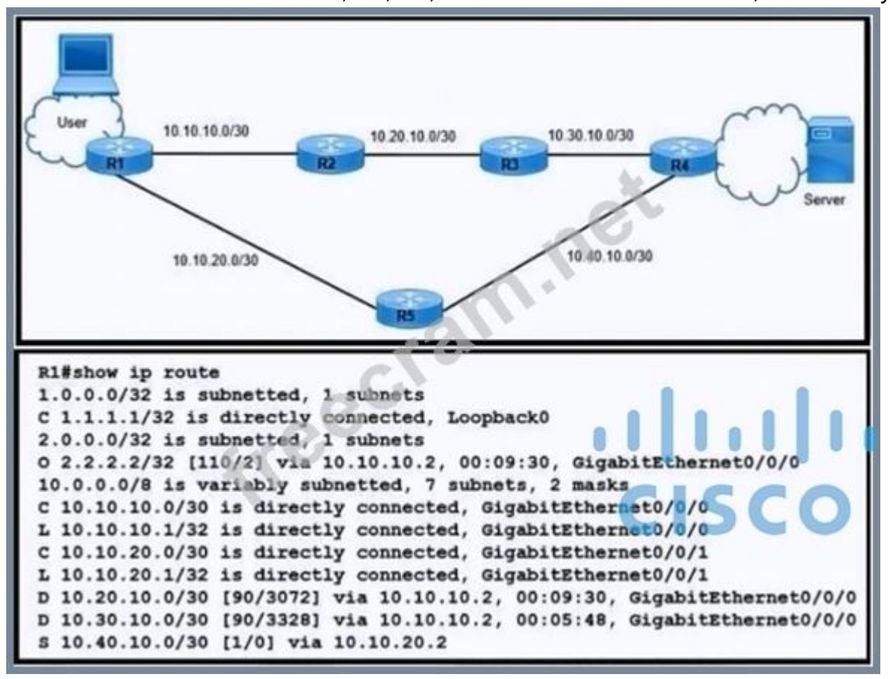
**NEW QUESTION: 97**
Refer to the exhibit. An engineer must configure router R101 for SSH access on ports 2001 through 2011. After the configuration, some expected ports were inaccessible. Which command resolves the issue?




**A.** ip ssh port 2001 rotary 1 11
line vty 0 4
transport input ssh
**B.** ip ssh port 2001 rotary 11
line vty 0 4
transport input telnet
**C.** ip ssh port 2000 rotary 1 11
line vty 0 4

transport input all
**D.** ip ssh port 2000 rotary 11
line vty 0 4
transport input ssh
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 98**
Refer to the exhibit. Routers R1, R2, R3, and R4 use EIGRP. However, traffic always prefers R1 to R5 backup links in nonfailure scenarios. Which configuration resolves the issue?




**A.** R1(config)#int gigabitEthernet 0/0/0
R1(config-if)#bandwidth 10000000
**B.** R1(config)#int gigabitEthernet 0/0/0
R1 (config-if)#bandwidth 10000
**C.** R1(config)#no ip route 10.40.10.0 255.255.255.252 10.10.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
**D.** R1(config)#no ip route 10.40.10.0 255.255.255.252 10.10.20.2
R1(config)#ip route 10.40.10.0 255.255.255.252 10.10.20.2 115
**Answer: (SHOW ANSWER)**
The issue occurs because EIGRP selects the best path based on the bandwidth and delay metrics. The backup link (R1 → R5) is being preferred due to its better metrics compared to the primary path (R1 → R2 → R3 → R4).
To resolve this, adjust the bandwidth on the interface connected to R5 (GigabitEthernet 0/0/0) to a lower value, such as 10000 kbps. By reducing the bandwidth, EIGRP calculates a higher metric for the link to R5, making it less preferable than the primary path through R2, R3, and R4. This ensures that traffic will use the primary path in nonfailure scenarios.

**NEW QUESTION: 99**

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

**A.** IPv6 Snooping

**B.** IPv6 Source Guard

**C.** IPv6 DAD Proxy

**D.** IPv6 RA Guard

**Answer: (SHOW ANSWER)**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-src-guard.html

**NEW QUESTION: 100**

How many labels are present in an MPLS Layer 3 packet traversing through the network without traffic engineering?



**A.** 1

**B.** 2

**C.** 3

**D.** 4

**Answer: (SHOW ANSWER)**

Explaination:

In MPLS (Multiprotocol Label Switching), when a Layer 3 packet traverses the network without traffic engineering, only one label is typically present. This label is used by the MPLS routers (label switch routers or LSRs) to forward the packet based on its label rather than the IP address.

**NEW QUESTION: 101**

Which two components are needed for a service provider to utilize the L3VPN 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)**

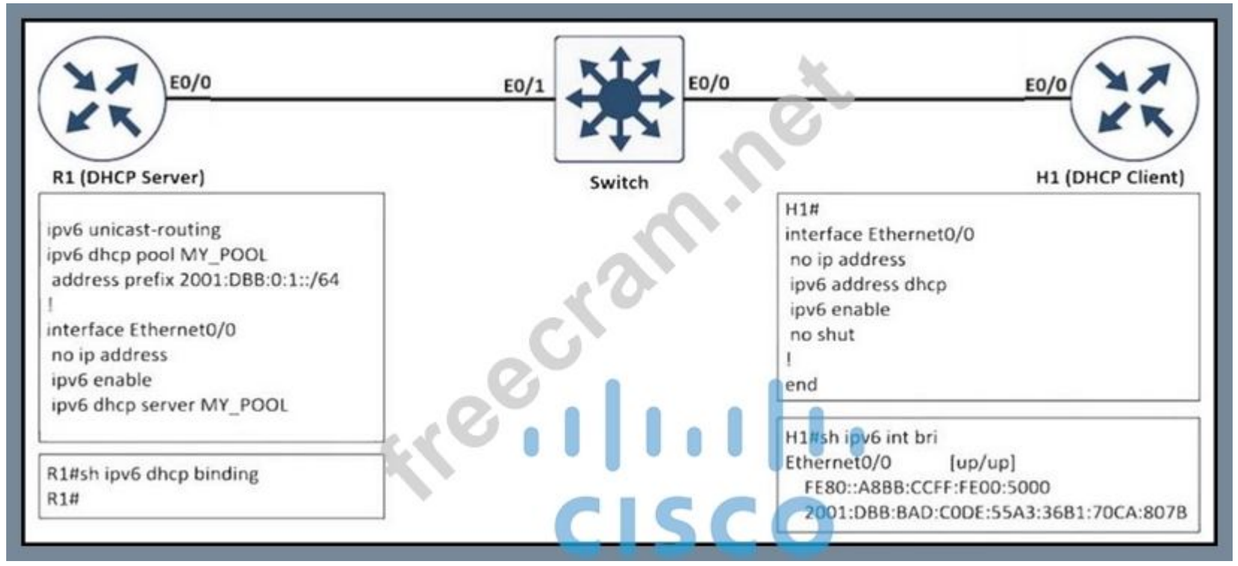
MPLS Network Protocols

+ 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: 102**

Refer to the exhibit. The client received the IPv6 address from the IPv6 DHCP server but the show command does not show the IPv6 DHCP bindings on the server. Which action resolves the issue?



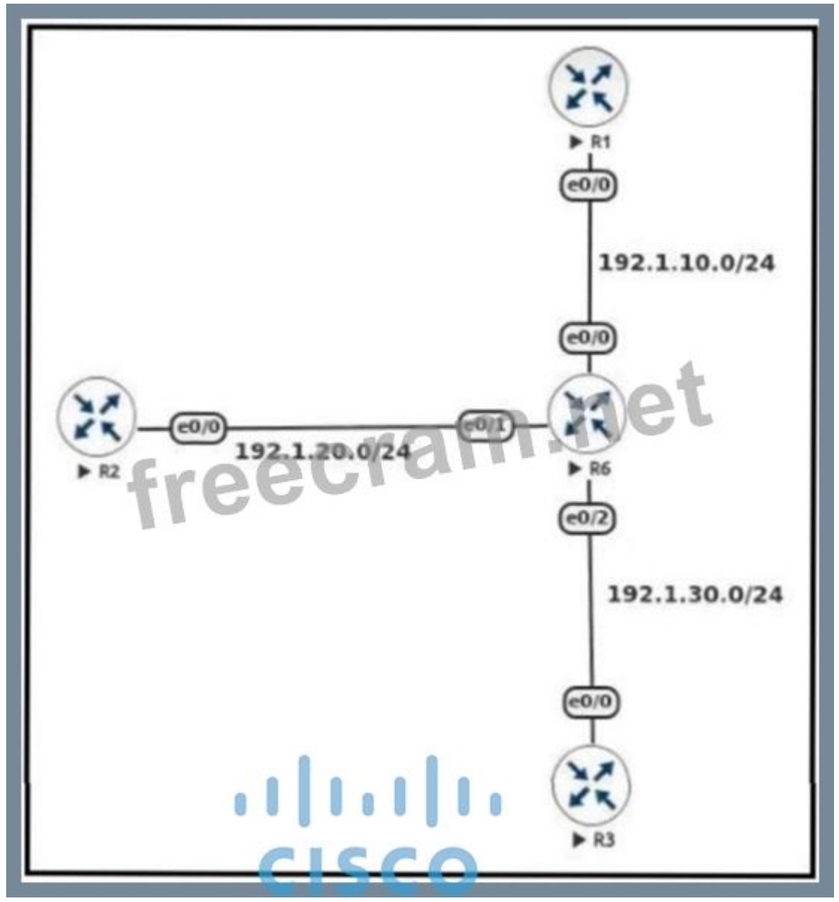

**A.** Configure H1 as the DHCP client that manually assigns the IPv6 address on interface e0/0.
**B.** Configure authorized DHCP servers to avoid IPv6 addresses from a rogue DHCP server.
**C.** Extend the DHCP lease time because R1 removed the IPv6 address earlier after the lease expired.
**D.** Use the 2001:DBB:BAD:CODE::/64 prefix for the DHCP pool on R1.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 103**
Which router translates the customer routing information into VPNv4 routes to exchange VPNv4 routes with other devices through MP-BGP?
**A.** CE
**B.** PE
**C.** VPNv4 RR
**D.** P
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 104**
The OSPF database of a router shows LSA types 1, 2, 7, and 3 default router only.
Which type of area is this router connected to?
**A.** NSSA
**B.** NSSA totally stub
**C.** stub area
**D.** totally stubby area
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 105**
Refer to the exhibit. An engineer must configure DMVPN Phase 3 hub-and-spoke topology to enable a spoke-to-spoke tunnel.

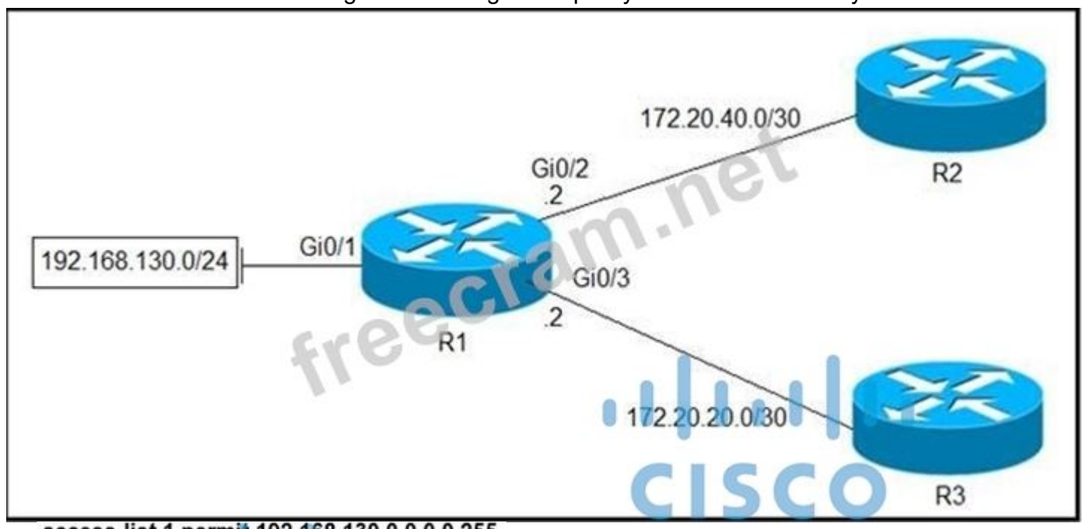
Which NHRP configuration meets the requirement on R6?




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

ip nhrp network-id 1
ip nhrp map 192.168.1.2 192.1.20.2
**D.** interface Tunnel1
ip nhrp authentication Cisco123
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp redirect
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 106**
Refer to the exhibit. Which configuration configures a policy on R1 to forward any traffic that is sourced from the 192.168.130.0/24 network to R2?




**A.**
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.2
```

**B.**
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.2
```

**C.**
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.1
```
**D.**
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.1
```

**Answer: (SHOW ANSWER)**

Look at the address of the local router (R1) on p2p links - it has .2, so it means the next hop (the remote router) is .1.



**NEW QUESTION: 107**

Refer to the exhibit. R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1.

What action will fix the issue?

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

**A.** Fix route dampening configured on the router.

**B.** Replace the SFP module because it is not supported.

**C.** Fix IP Event Dampening configured on the interface.

**D.** Correct the IP SLA probe that failed.

**Answer: (SHOW ANSWER)**

The log messages explicitly reference IF-EvD, which indicates IP Event Dampening on the interface. This feature is suppressing interface state transitions and is the reason the link is not operating normally. Correcting the IP Event Dampening configuration on GigabitEthernet0/0 restores stable connectivity between the routers.

**NEW QUESTION: 108**

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?

```
100.0.0.0/32 is subnetted, 3 subnets
C       100.1.1.1 is directly connected, Loopback0
D       100.2.2.2 [90/156160] via 10.1.1.2, 00:00:46, FastEthernet0/0
D       100.3.3.3 [90/158720] via 10.1.1.14, 00:00:44, FastEthernet1/0
                  [90/158720] via 10.1.1.2, 00:00:44, FastEthernet0/0
    10.0.0.0/8 is variably subnetted, 13 subnets, 4 masks
D       10.1.1.8/30 [90/30720] via 10.1.1.14, 00:00:44, FastEthernet1/0
C       10.1.1.12/30 is directly connected, FastEthernet1/0
C       10.1.1.0/30 is directly connected, FastEthernet0/0
D       10.1.1.4/30 [90/30720] via 10.1.1.2, 00:00:45, FastEthernet0/0
C       10.100.1.40/32 is directly connected, Loopback40
D EX    10.1.1.80/29 [170/33280] via 10.1.1.14, 00:00:45, FastEthernet1/0
                  [170/33280] via 10.1.1.2, 00:00:45, FastEthernet0/0
C       10.100.1.50/32 is directly connected, Loopback50
C       10.100.1.10/32 is directly connected, Loopback10
S       10.100.1.0/24 is a summary, 00:00:48, Null0
C       10.100.1.30/32 is directly connected, Loopback30
C       10.100.1.20/32 is directly connected, Loopback20
C       10.200.1.0/24 is directly connected, FastEthernet0/1
D EX    10.247.10.0/30 [170/2174976] via 10.1.1.14, 00:00:46, FastEthernet1/0
                  [170/2174976] via 10.1.1.2, 00:00:46, FastEthernet0/0
```

**A.** Remove the 10.100.1.0/24 static route.

**B.** Disable auto summarization on R1.

**C.** EIGRP on loopback Interfaces.

**D.** Redistribute connected routes into EIGRP Enable

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 109**

Refer to the exhibit. An engineer must filter EIGRP updates that are received to block all 10.10.10.0/24 prefixes. The engineer tests the distribute list and finds one associated prefix. Which action resolves the issue?

```
R1(config)#ip access-list standard EIGRP-FILTER
R1(config-std-nacl)#deny 10.10.10.0 0.0.0.0
R1(config-std-nacl)#permit 0.0.0.0 0.0.0.0
R1(config)#router eigrp 10
R1(config-router)#distribute-list route-map EIGRP in
!
R1(config)#route-map EIGRP permit 10
R1(config-route-map)#match ip address EIGRP-FILTER
!
R1#show ip route eigrp | include 10.10.10.
D      10.10.10.128/25
```

**A.** There is a permit in the route map that allows this prefix. A deny 20 statement is required with no match condition to block the prefix.

**B.** There is a permit in the ACL that allows this prefix into EIGRP. The ACL should be modified to deny 10.10.10.0 255.255.255.0.

**C.** There is a permit in the ACL that allows this prefix into EIGRP. The ACL should be modified to deny 10.10.10.0 0.0.0.255.

**D.** There is a permit in the route map that allows this prefix. A deny 20 statement is required with a match condition to match a new ACL that denies all prefixes.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 110**

You need to resolve a route-selection problem in a redistributed network by increasing the administrative distance to several networks for a protocol, other than EIGRP or BGP, so that these routes will not be used. You create access list 5 to identify the relevant networks, and access the routing protocol configuration prompt.
Which command will set the administrative distance to these networks to 220 for the selected protocol?

**A.** Router(config-router)# admin 220 access-list 5

**B.** Router(config-router)# increase 0.0.0.0 255.255.255.255 admin 220 list 5

**C.** Router(config-router)# distance 220 0.0.0.0 255.255.255.255 5

**D.** Router(config-router)# list 5 distance 220

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 111**

Refer to the exhibit. What is the result if applying this configuration?

```
R1#show policy-map control-plane
 Control Plane
        Service-policy input: CoPP-BGP
          Class-map: BGP (match all)
            2716 packets, 172071 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: access-group name BGP
            drop

          Class-map: class-default (match-any)
            5212 packets, 655966 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: any
```

**A.** The router can form BGP neighborships with any other device.

**B.** The router can form BGP neighborships with any device that matched by the access list named "BGP"

**C.** The router cannot form BGP neighborships with any other device

**D.** The router cannot form BGP neighborships with any device that is matched by the access list named "BGP"

**Answer: (SHOW ANSWER)**

https://tools.cisco.com/security/center/resources/protecting_border_gateway_protocol#13

**NEW QUESTION: 112**

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


**A.** Configure IOS control plane protection using ACL 90 on interface E1/0

**B.** Configure IOS management plane protection using ACL 90 on interface E1/0

**C.** Create an inbound ACL on interface E1/0 to deny SNMP from host 10.11.110.12

**D.** Add a permit statement including the host 10.11.110.12 into ACL 90

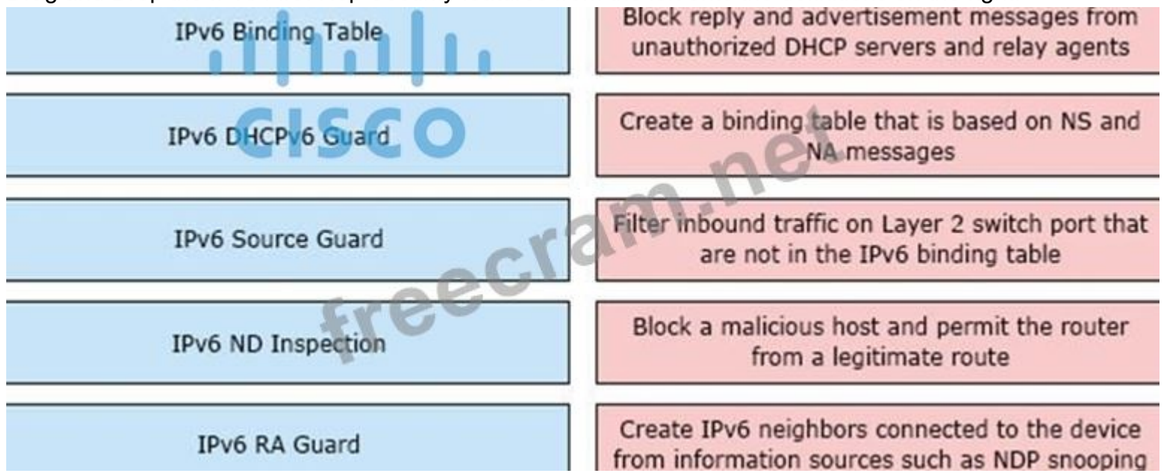
**Answer: (SHOW ANSWER)**

One of the best way to prevent unauthorized attempt to access SNMP is to use Access control list or ACLs. Use the inbound ACL on the interface and deny SNMP from the host that is accessing it without authorization.

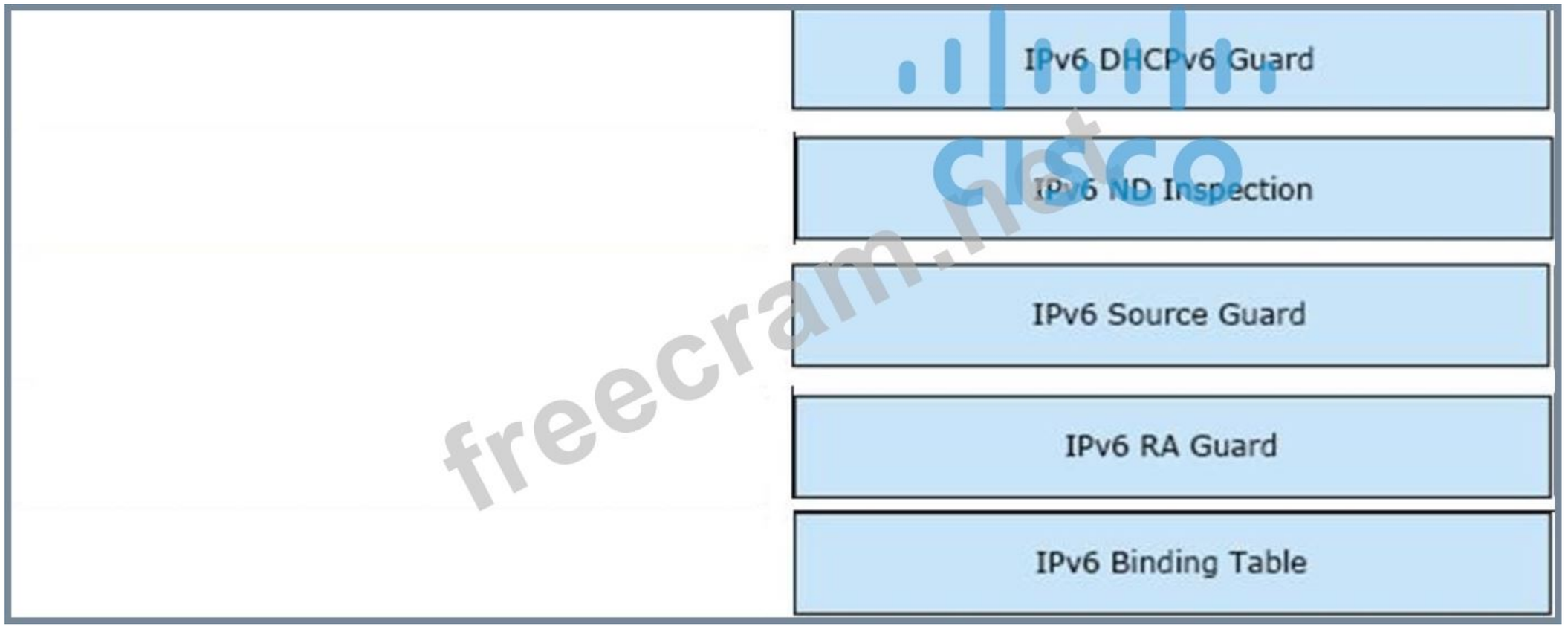
**NEW QUESTION: 113**

Drag and Drop Question

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




**Answer:**

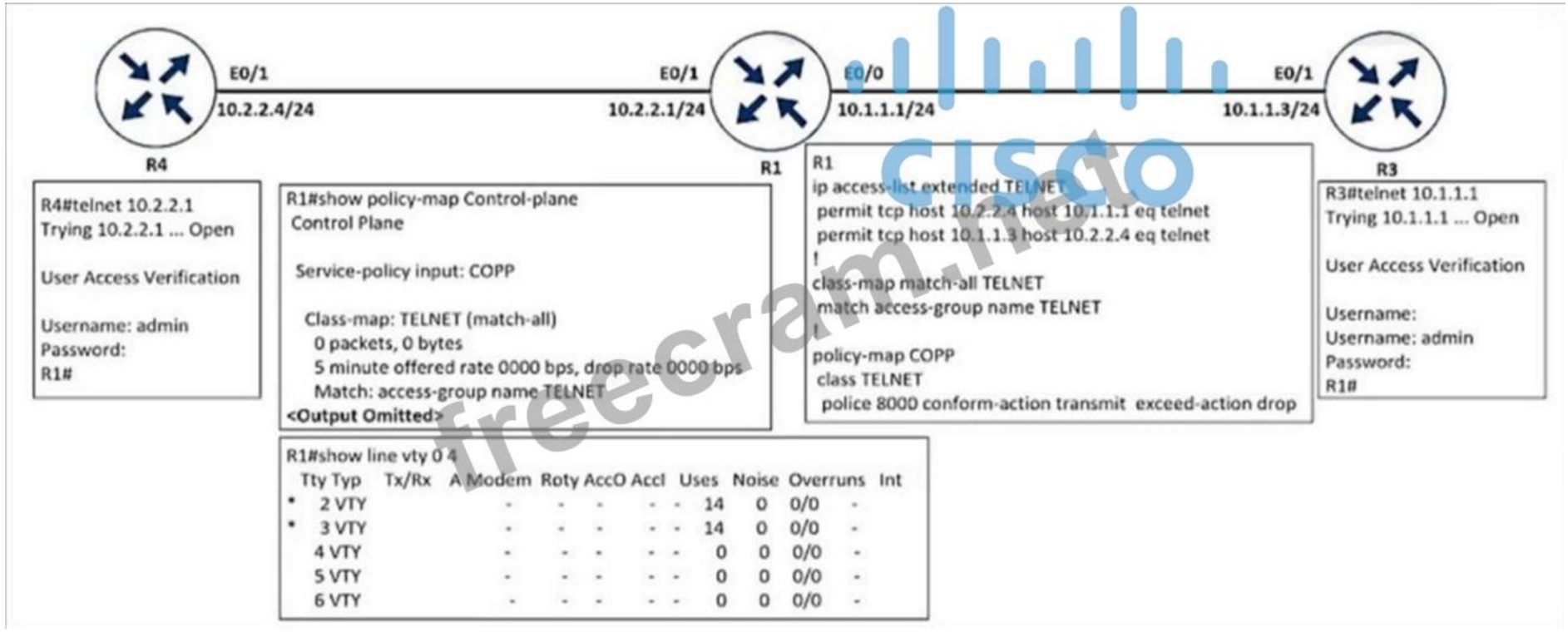



Explanation:
The DHCPv6 Guard feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients.
Client messages or messages sent by relay agents from clients to servers are not blocked.
IPv6 ND Inspection creates a binding table that is based on NS (Neighbor Solicitation) and NA (Neighbor Advertisement) messages. The switch then uses this table to check any future NS/NA messages. When the IPv6-LLA combination does not match, it drops the message. This only applies to NS/NA messages, it doesn't drop any actual data packets that have a spoofed IPv6 or MAC address.
IPv6 Source Guard filters inbound traffic on L2 switch ports that are not in the IPv6 binding table.
The binding table stores the following information:
+ IPv6 address
+ MAC address
+ VLAN
+ Interface ID
Source Guard only looks at information found in the binding table, and it doesn't fill the binding table.
The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices.

**NEW QUESTION: 114**
Which of the following are valid DHCP options that DHCP servers can be configured to use with DHCP clients when offering a lease? (Choose two.)
**A.** DHCP Option 4: Client host name

**B.** DHCP Option 6: DNS servers
**C.** DHCP Option 3: Lease Duration
**D.** DHCP Option 1: subnet mask
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 115**
Refer to the exhibit. An engineer implemented CoPP to limit Telnet traffic to protect the router CPU. It was noticed that the Telnet traffic did not pass through CoPP.
Which configuration resolves the issue?

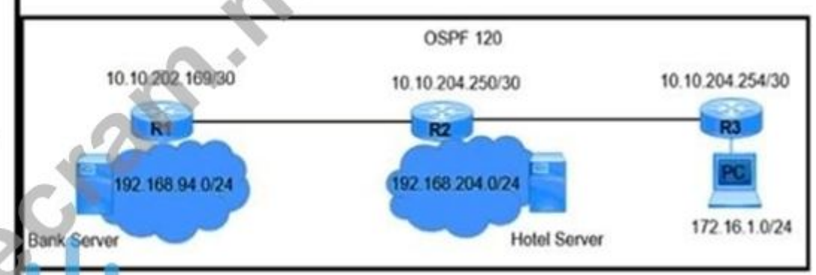



**A.** policy-map COPP
class TELNET
police 8000 conform-action transmit exceed-action transmit
**B.** policy-map COPP
class TELNET
police 8000 conform-action transmit exceed-action transmit violate-action drop
**C.** ip access-list extended TELNET
permit tcp host 10.2.2.1 host 10.2.2.4 eq telnet
permit tcp host 10.1.1.1 host 10.1.1.3 eq telnet
**D.** ip access-list extended TELNET
permit tcp host 10.2.2.4 host 10.2.2.1 eq telnet
permit tcp host 10.1.1.3 host 10.1.1.1 eq telnet

**Answer: (SHOW ANSWER)**
To avoid matching the filtering and policing that are configured in a subsequent class, configure policing in each class. CoPP does not apply the filtering in a class that does not contain a police command. A class without a police command matches no traffic.

**NEW QUESTION: 116**
Refer to the exhibit. A network engineer finds that PC1 is accessing the hotel website to do the booking but fails to make payment. Which action resolves the issue?

```
R3# show ip ospf database router 10.10.202.169
OSPF Router with ID (10.10.204.254) (Process ID 120)
Router Link States (Area 0)
    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 192.168.94.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metrics: 100

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.10.202.168
     (Link Data) Network Mask: 255.255.255.252
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

R3# show ip route 10.10.202.168
Routing entry for 10.10.202.168/30
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 172.16.1.26
      Route metric is 0, traffic share count is 1
```




**A.** Configure a reverse route on R1 for PC1 172.16.1.0/24.
**B.** Decrease the AD to 5 OSPF route 192.168.94.0 on R1.
**C.** Increase the AD to 200 of static route 192.168.94.0 on R3.
**D.** Allow stub network 10.10.202.168/30 on router R3 OSPF.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 117**
Refer to the exhibit. 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)**
Mismatched AS Numbers
When you enter the debug eigrp packets hello command, it reveals that the router does not receive the Hello packets.
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol- eigrp/118974-technote-eigrp-00.html#anc36

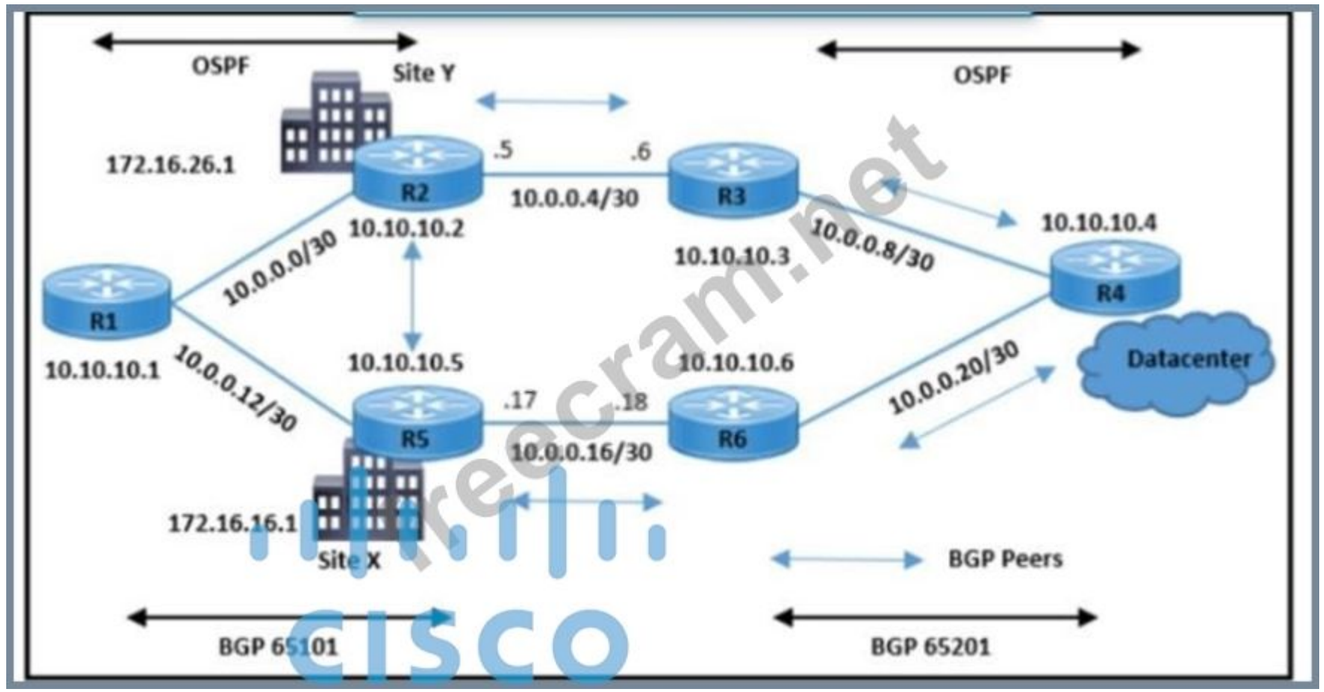
**NEW QUESTION: 118**
Out of the below options regarding DMVPN & FLEXVPN, select the correct one.
**A.** FlexVPN uses a new key management protocol - IKEv2, while most traditional DMVPN networks use IKEv1
**B.** FlexVPN uses a new key management protocol - IKEv1, while most traditional DMVPN networks use IKEv2
**C.** Flex VPN & DMVPN both are supported only on Firewalls.
**D.** With FlexVPN there's multiple standard way of NHRP and routing protocols operations as opposed to 1 phase of DMVPN
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 119**
You have a DNA center deployed in your environment. Which feature of the DNA Center will you use for system-guided as well as self-guided troubleshooting.
**A.** Automation
**B.** Discovery
**C.** Zero Trust

**D.** Assurance
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 120**
Refer to the exhibit. A customer reports a failure and intermittent disconnection between two office buildings, site X and site Y. The network team determines that both sites are exchanging email application traffic with the data center network. Which configuration resolves the issue between site X and site Y?

```
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
```




**A.** R2(config-router)#neighbor 10.10.10.5 update-source loopback 0
R2(config)#router bgp 65101
**B.** R2(config-router)#neighbor 10.10.10.5 next-hop-self
R2(config)#router bgp 65101
**C.** R2(config-router)#no timers bgp 3 15
R2(config)#router bgp 65101
**D.** R5(config-router)#neighbor 10.10.10.2 next-hop-self
R5(config)#router bgp 65101
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 121**
Refer to the exhibit. While troubleshooting an EIGRP neighbor adjacency problem, the network engineer notices that the interface connected to the neighboring router is not participating in the EIGRP process. Which action resolves the issue?

```
Router#show ip eigrp interfaces
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
Lo0                0      0/0          0/0          0     0/0          0           0
Fa0/0              1      0/0          0/0          7     0/2          50          0

Router#show running-config | section eigrp
router eigrp 1
 network 172.16.0.0 0.0.0.255
 network 192.168.2.2 0.0.0.0
 network 192.168.12.2 0.0.0.0

Router#show running-config interface Fa0/3
Building configuration...


Current configuration : 93 bytes
!
interface FastEthernet0/3
 ip vrf forwarding CLIENT1
 ip address 172.16.0.1 255.255.255.0
```

**A.** Configure EIGRP metrics on interface FastEthemet0/3.
**B.** Configure the network command under EIGRP address family vrf CLIENT1.
**C.** Configure the network command under EIGRP address family ipv4.
**D.** Configure the network command to network 172.16.0.1 0.0.0.0.
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 122**
Which command displays the IP routing table information that is associated with VRF-Lite?
**A.** Show ip vrf
**B.** Show ip route vrf
**C.** Show run vrf
**D.** Show ip protocols vrf
**Answer: (SHOW ANSWER)**
https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/software/15_4_1_cg/vrf_cgr1000.html
show ip route vrf vrf-name [ connected ] [ protocol [ as- Displays IP routing table number ] [ list

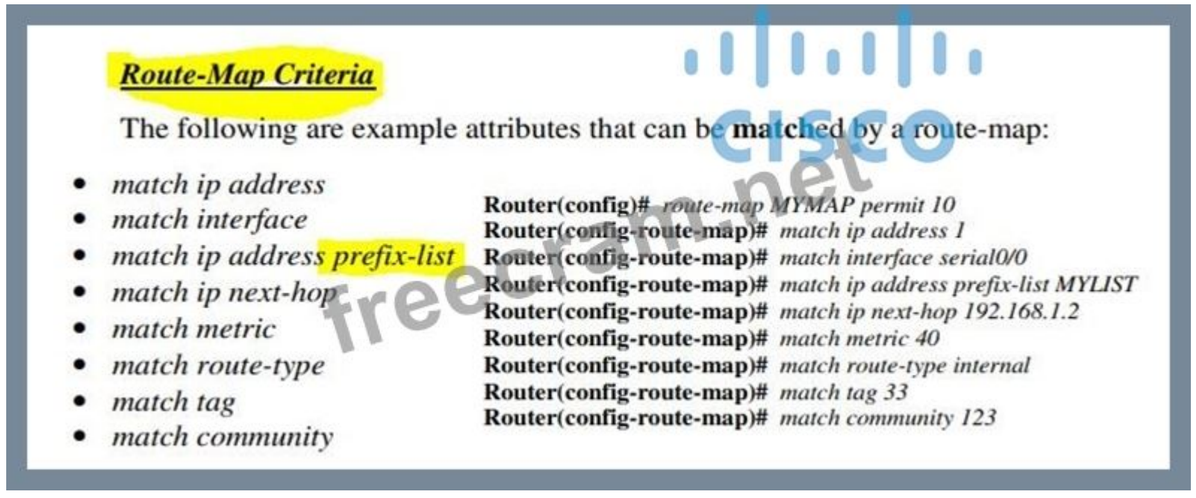
[ list-number ]] [ mobile ] [ odr ] [ profile ] information associated [ static ] [ summary ][ supernets- only ] with a VRF.

**NEW QUESTION: 123**
Refer to the exhibit. The network administrator configured redistribution on an ASBR to reach to all WAN networks but failed. Which action resolves the issue?

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



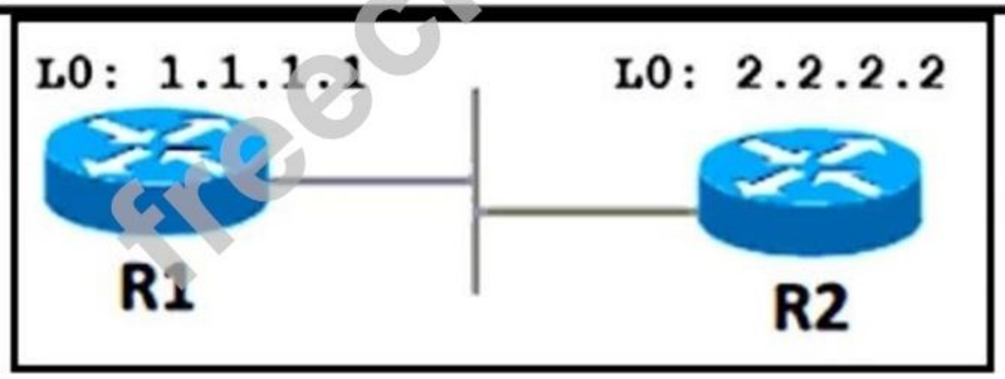
**A.** The route map must have the keyword prefix-list to evaluate the prefix list entries
**B.** The OSPF process must have a metric when redistributing prefixes from EIGRP.
**C.** The route map EIGRP->OSPF must have the 10.0.106.0/24 entry to exist in one of the three prefix lists to pass
**D.** EIGRP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




**NEW QUESTION: 124**
A time based access list has been configured on R1 to allow SSH access to the device only on weekdays. Which of the following are valid options when using the time range command? (Choose two.)
**A.** recurring
**B.** relative
**C.** absolute
**D.** periodic
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 125**
Refer to the exhibit. R1 cannot establish a neighbor relationship with R2. Which action resolves the issue?

```
R1#debug ip ospf adj
23:42:08.259: OSPF: Send DBD to 2.2.2.2 on Ethernet0/0 seq 0x836 opt 0x52 flag 0x7 len 32
23:42:08.339: OSPF: Rcv DBD from 2.2.2.2 on Ethernet0/0 seq 0x836 opt 0x52 flag 0x7 len
32 mtu 1532 state EXSTART


R2#debug ip ospf adj
23:42:08.423: OSPF: Send DBD to 1.1.1.1 on Ethernet0/0 seq 0x836 opt 0x52 flag 0x7 len 32
23:42:08.423: OSPF: First DBD and we are not SLAVE
23:42:08.511: OSPF: Rcv DBD from 1.1.1.1 on Ethernet0/0 seq 0x836 opt 0x52 flag 0x2 len
52 mtu 1500 state EXSTART
```




**A.** Configure the neighbor 2.2.2.2 command on R1 under the OSPF process.
**B.** Configure the ip ospf network broadcast command on the interfaces of R1 and R2.
**C.** Configure the mtu ignore command on the interfaces of R1 and R2.
**D.** Configure the ip ospf network point-to-point command on the interfaces of R1 and R2.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 126**
Which task do you need to perform first when you configure IP SLA to troubleshoot a network connectivity issue?
**A.** Enable the ICMP echo operation
**B.** Verify the ICMP echo operation
**C.** Schedule the ICMP echo operation
**D.** Specify the test frequency
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 127**
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: 128**
Refer to the exhibit. The network administrator configured VRF lite for customer A. The technician at the remote site misconfigured VRF on the router. Which configuration will resolve connectivity for both sites of customer a?

**Router Configuration:**

```
ip vrf customer_a
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
!
interface FastEthemet0.1
 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
```

A.

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

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

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

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

**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: 129**

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?

```
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
```

**A.** Configure SNMP interface index persistence on the router.

**B.** Save the router configuration to startup-config before reloading the router.

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

**D.** Configure SNMP to use static OIDs referring to individual router interfaces.

**Answer: (SHOW ANSWER)**

https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_boo k/ifindx.pdf

**NEW QUESTION: 130**

Refer to the exhibit. An engineer configured NetFlow to capture traffic information through the router, but it is not working as expected. Which action captures the flow information from this router to the collector?

```
flow exporter EXPORTER-1
 destination 172.16.10.2
 export-protocol netflow-v9
 transport udp 90
 exit
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v4_r1
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

**A.** Change the interface configuration FLOW-MONITOR-1 from input to output.

**B.** Configure a flow exporter under flow FLOW-MONITOR-1.

**C.** Configure more than one flow exporter destination addresses.

**D.** Change the flow exporter transport protocol from UDP to TCP

**Answer: (SHOW ANSWER)**

To fix the issue, the engineer must configure the flow exporter under the flow monitor. This can be achieved by adding the following command under the flow monitor FLOW-MONITOR-1 configuration:

flow monitor FLOW-MONITOR-1

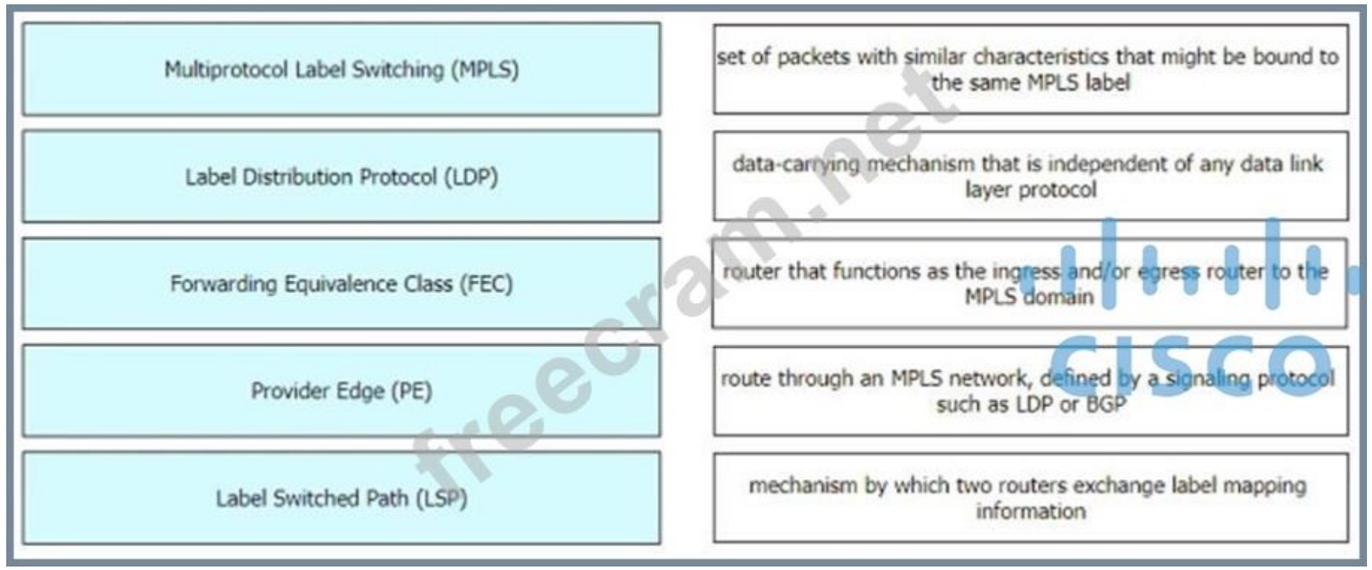
exporter EXPORTER-1

This links the flow monitor to the exporter and allows the collected data to be sent to the NetFlow collector.

**NEW QUESTION: 131**

Drag and Drop Question

Drag and drop the terminology from the left onto the corresponding definitions on the right.

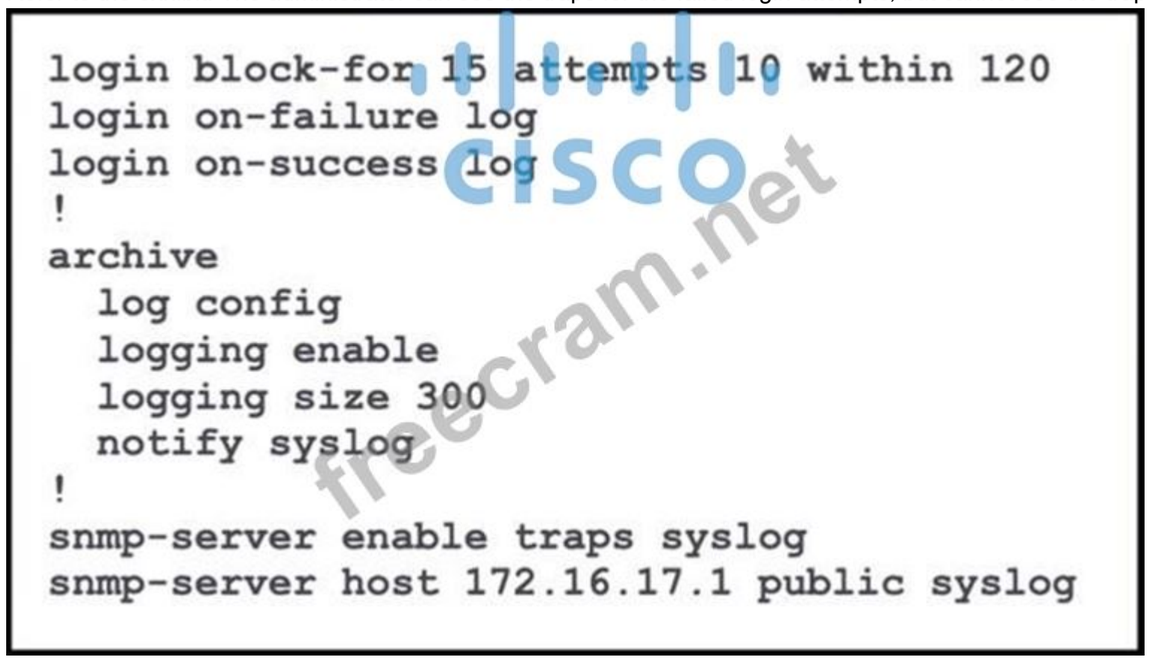



**Answer:**


**NEW QUESTION: 132**
Which two protocols work in the control plane of P routers across the MPLS cloud? (choose two)
**A.** MPLS OAM
**B.** LDP
**C.** LSP
**D.** RSVP
**E.** ECMP

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 133**
Refer to the exhibit. The administrator can see the traps for the failed login attempts, but cannot see the traps of successful login attempts. What command is needed to resolve the issue?




**A.** Configure logging history 2
**B.** Configure logging history 3
**C.** Configure logging history 4
**D.** Configure logging history 5
**Answer: (SHOW ANSWER)**
By default, the maximum severity sent as a syslog trap is warning. That is why you see syslog traps for login failures. Since a login success is severity 5 (notifications), those syslog messages will not be converted to traps.
To fix this, configure:

**logging history 5**

Syslog levels are listed below

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



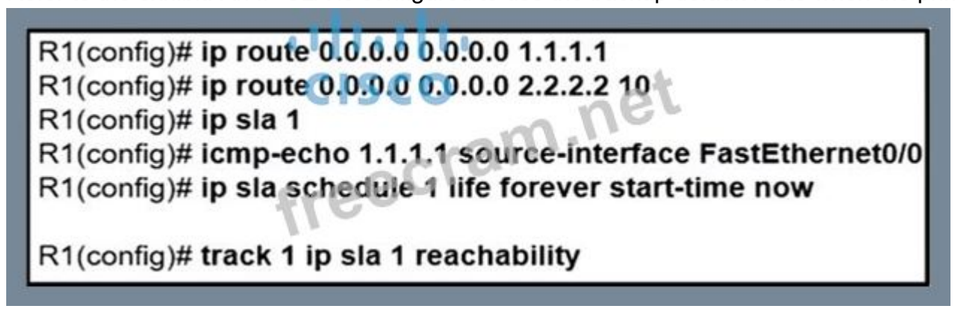
Note:
The syntax of login block is:
login block-for seconds attempts tries within seconds

**NEW QUESTION: 134**
Which of the following statements are true regarding two EIGRP routers to become neighbors?
**A.** Must have identical hello and dead timers
**B.** Must utilize unique router ID's
**C.** Must have matching MTU's on the physical network links that connect the routers.
**D.** Must use the same ASN.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 135**
What is an MPLS LDP targeted session?
**A.** LDP session established by exchanging multicast hello packets
**B.** LDP session established between LSRs by exchanging TCP hello packets
**C.** session between neighbors that are connected no more than one hop away

**D.** label distribution session between non-directly connected neighbors
**Answer: D (LEAVE A REPLY)**

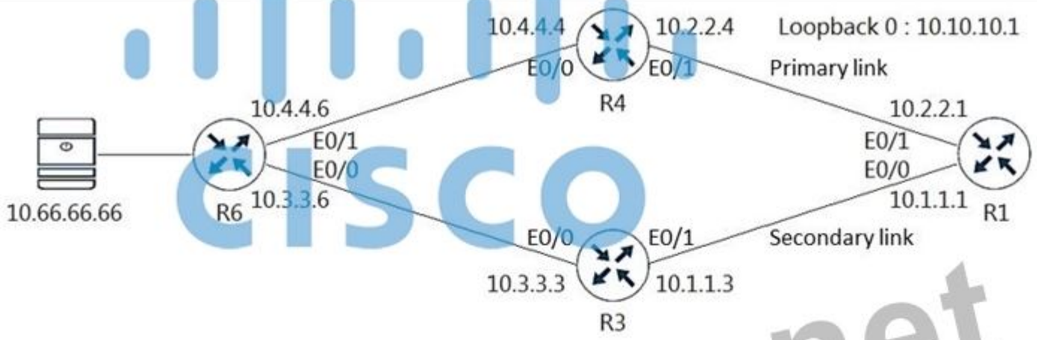
**NEW QUESTION: 136**
Refer to the exhibit. An IP SLA is configured to use the backup default route when the primary is down, but it is not working as desired. Which command fixes the issue?




**A.** R1(config)# ip route 0.0.0.0.0.0.0.2.2.2.2 10 track 1
**B.** R1(config)# ip route 0.0.0.0.0.0.0.2.2.2.2
**C.** R1(config)#ip sla track 1
**D.** R1(config)# ip route 0.0.0.0.0.0.0.1.1.1.1 track 1
**Answer: (SHOW ANSWER)**
Note: By default Static Router AD value-1 hence ip route 0.0.0.0. 0.0.0.0. 1.1.1.1 track 1 means AD-1 which must be less than of back up route AD.
Define the backup route to use when the tracked object is unavailable. !--- The administrative distance of the backup route must be greater than !--- the administrative distance of the tracked route. !--- If the primary gateway is unreachable, that route is removed !--- and the backup route is installed in the routing table !--- instead of the tracked route.
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default- routes-using-I.html
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation- firewalls/118962-configure-asa-00.html



**NEW QUESTION: 137**
Refer to the exhibit. An engineer configured NetFlow but cannot receive the flows from R1. Which two configurations resolve the issue? (Choose two)




```
R3# & R4#
interface Ethernet0/1
 ip access-group DDOS in
!
ip access-list extended DDOS
 permit tcp any any
 deny  udp any any range 1024 65535
 permit ip any any
```

```
R1#sh flow interface
Interface Ethernet0/0
  FNF: monitor: FlowMonitor1
      direction:   Input
      traffic(ip):  on
  FNF: monitor: FlowMonitor1
      direction:   Output
      traffic(ip):  on
Interface Ethernet0/1
  FNF: monitor: FlowMonitor1
      direction:   Input
      traffic(ip):  on
  FNF: monitor: FlowMonitor1
      direction:   Output
      traffic(ip):  on
```

```
R1#show flow exporter
Flow Exporter FlowExporter1:
  Description: User defined
  Export protocol: NetFlow Version 5
  Transport Configuration:
    Destination IP address: 10.66.66.66
    Source IP address:        10.1.1.1
    Transport Protocol:       UDP
    Destination Port:         1090
    Source Port:      54186
    DSCP:             0x0
    TTL:              255
    Output Features: Not Used
```

```
R1#show flow monitor
Flow Monitor FlowMonitor1:
  Description: User defined
  Flow Record: netflow ipv4 original-input
  Flow Exporter: FlowExporter1
  Cache:
    Type:      normal
    Status:    allocated
    Size:      4096 entries / 344088 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
    Synchronized Timeout:    600 secs
```



**A.** R3(config)#flow exporter FlowExporter1
R3(config-flow-exporter)#destination 10.66.66.66
**B.** R4(config)#flow exporter FlowExporter1
R4(config-flow-exporter)#destination 10.66.66.66
**C.** R4(config)#ip access-list extended DDOS
R4(config-ext-naci)#5 permit udp any host 10.66.66.66 eq 1090
**D.** R1(config)#flow exporter FlowExporter1
R1(config-flow-exporter)#destination 10.66.60.66
**E.** R3(config)#ip access-list extended DDOS
R3(config-ext-nacl)#5 permit udp any host 10.66.66.66 eq 1090
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 138**
Refer to the exhibit. Which action restores OSPF adjacency between R1 and R2?

```
R2#show running-config | section ospf
 ip ospf l area 1
 ip ospf l area 1
router ospf 1
 log-adjacency-changes
 area i stub no-summary
R2#show ip ospf interface brief
Interface    PID   Area  IP Address/Mask    Cost  State Nbrs  F/C
Lo0          1     1     10.0.0.2/32        1     Loop  0/0
Fa0/0        1     1     10.10.10.1/30      1     DR    0/1
R2#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 116 bytes
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.252
 ip mtu 1400
 ip ospf1 area 1
 duplex full
end

R2#show ip ospf neighbor

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

```
R1#show running-config | section ospf
 ip ospf l area o
 ip ospf l area 1
router ospf 1
 log-adjacency-changes
 area 1 stub no-summary
R1#show ip ospf interface brief
Interface    PID   Area  IP Address/Mask    Cost  State Nbrs  F/C
Lo0          1     0     10.0.0.1/32        1     LOOP  0/0
Lo0          1     1     10.10.10.2/30 Fal/o 1     BDR   0/1
R1#show running-config interface fastEthernet 1/0
Building configuration...

Current configuration : 115 bytes
!
interface FastEthernet1/0
 ip address 10.10.10.2 255.255.255.252
 ip ospf1 area 1
 duplex auto
  speed auto
end

R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address         Interface
10.10.10.1 R1#   1     EXCHANGE/DR     00:00:39    10.10.10.1      FastEthernet1/0
```

**A.** Change the IP MTU of R2 Fa0/0 to 1500
**B.** Change the IP MTU of R1 Fa1/0 to 1500
**C.** Change the IP MTU of R2 Fa0/0 to 1300
**D.** Change the IP MTU of R1 Fa1/0 to 1300
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 139**
Refer to the exhibit. R1 and R2 are configured as eBGP neighbor, R1 is in AS100 and R2 is in AS200. R2 is advertising these networks to R1:
172.16.16.0/20
172.16.3.0/24
172.16.4.0/24
192.168.1.0/24
192.168.2.0/24
172.16.0.0/16
The network administrator on R1 must improve convergence by blocking all subnets of
172.16.0.0/16 major network with a mask lower than 23 from coming in.
Which set of configurations accomplishes the task on R1?
**A.** ip prefix-list PL-1 deny 172.16.0.0/16 ge 23

ip prefix-list PL-1 permit 0.0.0.0/0 le 32
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 prefix-list PL-1 in
**B.** ip prefix-list PL-1 deny 172.16.0.0/16
ip prefix-list PL-1 permit 0.0.0.0/0
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 prefix-list PL-1 in
**C.** ip prefix-list PL-1 deny 172.16.0.0/16 le 23
ip prefix-list PL-1 permit 0.0.0.0/0 le 32
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 prefix-list PL-1 in
**D.** access-list 1 deny 172.16.0.0 0.0.254.255
access-list 1 permit any
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 distribute-list 1 in
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 140**
Refer to the exhibit. An administrator is configuring a GRE tunnel to establish an EIGRP neighbor to a remote router. The other tunnel endpoint is already configured. After applying the configuration as shown, the tunnel started flapping. Which action resolves the issue?

```
R2(config) # int tun0

*Feb 23 00:42:06.179: $LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down

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

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

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

*Feb 23 00:43:05.730: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.12.1 (Tunnel0) is up: new adjacency
*Feb 23 00:43:05.993: %ADJ-5-PARENT: Midchain parent maintenance
for IP midchain out of Tunnel0 - looped chain attempting to
stack
*Feb 23 00:43:15.193: %TUN-5-RECURDOWN: Tunnel0 temporarily
disabled due to recursive routing
*Feb 23 00:43:15.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down
```

**A.** Modify the network command to use the Tunnel0 interface netmask

**B.** Advertise the Loopback0 interface from R2 across the tunnel

**C.** Stop sending a route matching the tunnel destination across the tunnel

**D.** Readdress the IP network on the Tunnel0 on both routers using the /31 netmask

**Answer: (SHOW ANSWER)**

In this question we are advertising the tunnel IP address 192.168.12.2 to the other side. When other end receives the EIGRP advertisement, it realizes it can reach the other side of the tunnel via EIGRP. In other words, it reaches the tunnel destination through the tunnel itself -> This causes "recursive routing" error.

Note: In order to avoid this error, do not advertise the tunnel destination IP address on the tunnel interface to other side.

https://networklessons.com/cisco/ccie-routing-switching/gretunnel-recursive-routing-error

**NEW QUESTION: 141**

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

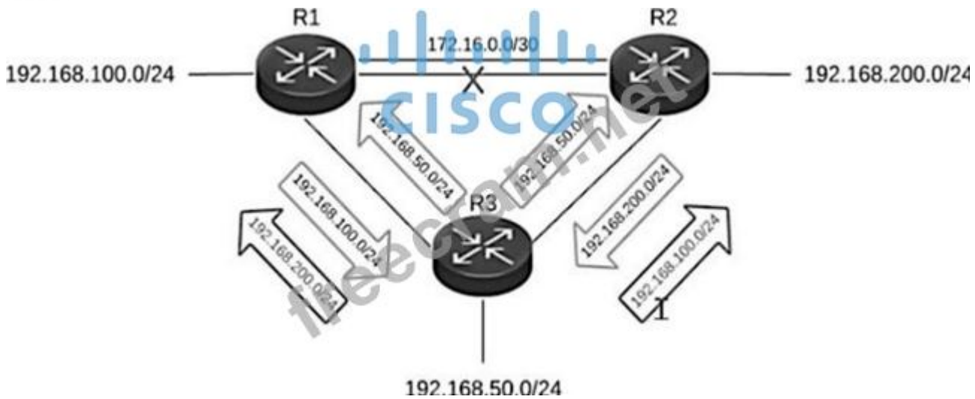
**C.** BOOTP port 68

**D.** DHCP option 69

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 142**
Refer to the exhibit. The primary link between R1 and R2 went down, but R3 is still advertising the 192.168.200.0/24 network to R1 and the 192.168.100.0/24 network to R2, which creates a loop. Which action resolves the issue?




**A.** Configure the summary-address 192.168.0.0 255.255.0.0 100 command on R3.
**B.** Configure the eigrp stub command under the EIGRP process on R2.
**C.** Configure the eigrp stub command under the EIGRP process on R3.
**D.** Configure the eigrp stub leak-map command under the EIGRP process on R1.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 143**
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: 144**
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?

```
Router#show running-config | include ip route
ip route 192.168.2.2 255.255.255.255 209.165.200.225 130
Router#show ip route

<output omitted>

Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopback0
      192.168.2.0/32 is subnetted, 1 subnets
O        192.168.2.2[110/11] via 192.168.12.2, 00:52:09, Ethernet0/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/24 is directly connected, Ethernet0/1
         209.165.200.226/32 is directly connected, Ethernet0/1
```

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

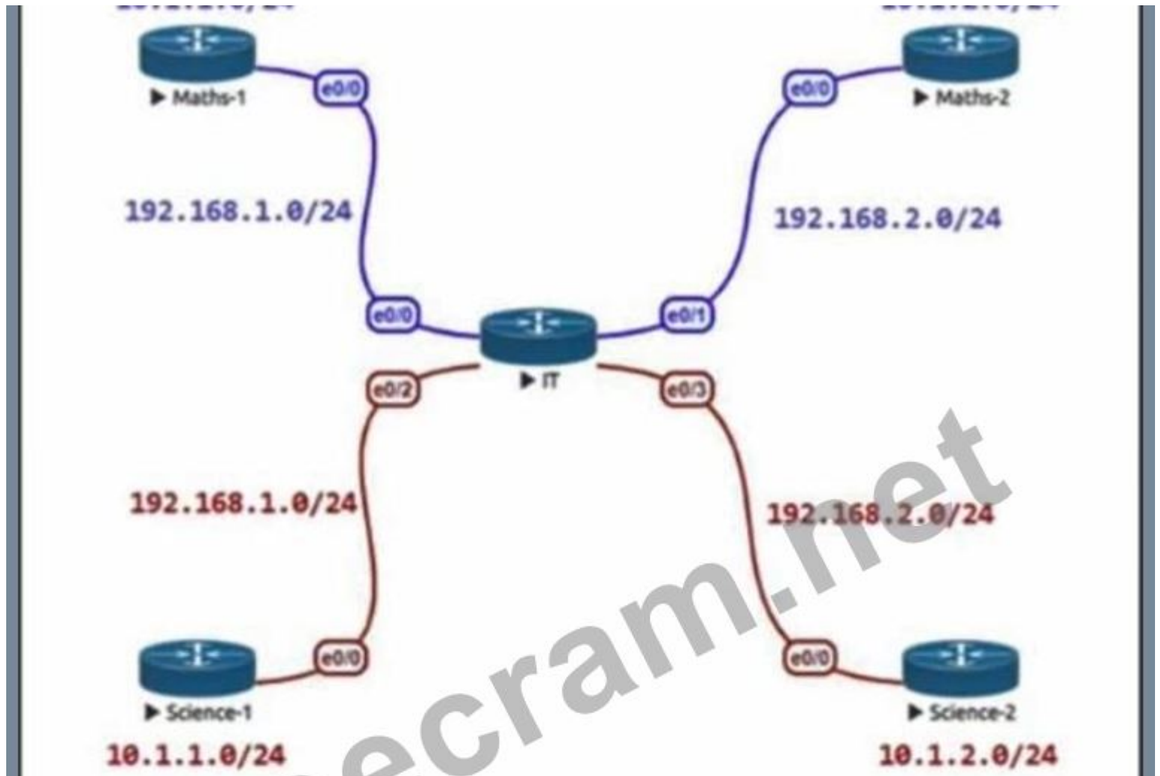
**NEW QUESTION: 145**
Which traffic does the following configuration allow?
ipv6 access-list cisco
permit ipv6 host 2001:DB8:0:4::32 any eq ssh
line vty 0 4
ipv6 access-class cisco in
**A.** all traffic to vty 0 4 from source 2001:DB8:0:4::32
**B.** only ssh traffic to vty 0 4 from source all
**C.** only ssh traffic to vty 0 4 from source 2001:DB8:0:4::32
**D.** all traffic to vty 0 4 from source all

**Answer: (SHOW ANSWER)**
Here we see that the Ipv6 access list called "cisco" is being applied to incoming VTY connections to the router. Ipv6 access list has just one entry, which allows only the single Ipv6 IP address of 2001:DB8:0:4::32 to connect using SSH only.

**NEW QUESTION: 146**
An engineer configured VRF-Lite on a router for VRF blue and VRF red. OSPF must be enabled on each VRF to peer to a directly connected router in each VRF. Which configuration forms OSPF neighbors over the network 10.10.10.0/28 for VRF blue and 192.168.0.0/30 for VRF red?
**A.** router ospf 1 vrf blue
network 10.10.10.0 0.0.0.252 area 0
router ospf 2 vrf red
network 192.168.0.0 0.0.0.240 area 0
**B.** router ospf 1 vrf blue
network 10.10.10.0 0.0.0.3 area 0
router ospf 2 vrf red
network 192 168.0.0 0.0.0.15 are 0
**C.** router ospf 1 vrf blue
network 10.10.10.0 0.0.0.15 area 0
router ospf 2 vrf red
network 192.168.0.0 0.0.0.3 area 0
**D.** router ospf 1 vrf blue
network 10.10.10.0 0.0.0.240 area 0
router ospf 2 vrf red
network 192.168.0.0 0.0.0.252 area 0
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 147**
Which transport layer protocol is used to form LDP sessions?
**A.** UDP
**B.** SCTP
**C.** TCP
**D.** RDP
**Answer: C (LEAVE A REPLY)**
LDP uses TCP as a reliable transport for sessions. When multiple LDP sessions are required between two LSRs, there is one TCP session for each LDP session.
Reference: https://tools.ietf.org/html/rfc5036

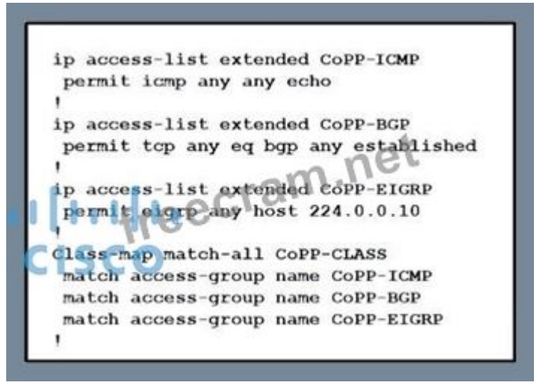
**NEW QUESTION: 148**
Refer to the exhibit. The IT router has been configured with the Maths VRF and the interfaces have been assigned to the VRF. Which set of configurations exchanges routes between the Maths-1 and Maths-2 routers using OSPF in area 0?


```
vrf definition Maths
 address-family ipv4
!
Interface E 0/0
 Vrf forwarding Maths
 Ip address 192.168.1.1 255.255.255.0
 No shut
!
Interface E 0/1
 Vrf forwarding Maths
 Ip address 192.168.2.1 255.255.255.0
 No shut
```

**A.** router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
**B.** router ospf 1 vrf Maths area 0
network 192.168.1.0
network 192.168.2.0
**C.** router ospf1
address-family ipv4 vrf Maths
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
**D.** router ospf 1 vrf Maths
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
**Answer: D (LEAVE A REPLY)**
In some Cisco IOS versions, router ospf 1 vrf Maths with the network command syntax directly under the VRF context is supported and correctly assigns the networks to the specified VRF and area.
Chosen option is directly specifies the VRF in the router ospf 1 vrf Maths command.

**NEW QUESTION: 149**
Refer to the exhibit. A CoPP policy is implemented to allow specific control traffic, but the traffic is not matching as expected and is getting unexpected behavior of control traffic. Which action resolves the issue?

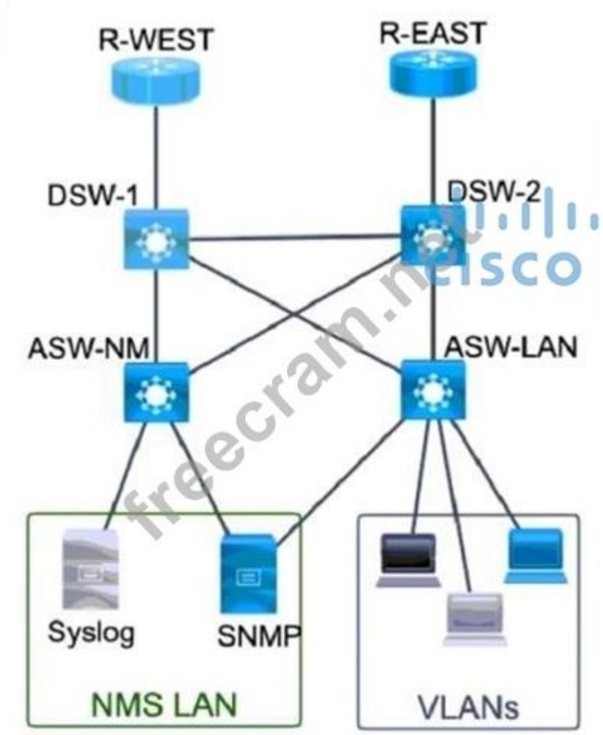



**A.** Use match-any instruction in class-map.
**B.** Create a separate class map against each ACL.
**C.** Use default-class to match ICMP traffic.
**D.** Create a separate class map for ICMP traffic.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 150**
LAB SIMULATION 8
Guidelines
This is a lab item in which tasks will be performed on virtual devices.
* Refer to the Tasks tab to view the tasks for this lab item.
* Refer to the Topology tab to access the device console(s) and perform the tasks.

* Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
* All necessary preconfigurations have been applied.
* Do not change the enable password or hostname for any device.
* Do not replace existing routing policies or configurations.
* Save your configurations to NVRAM before moving to the next item.
* Click Next at the bottom of the screen to submit this lab and move to the next question.
* When Next is clicked, the lab closes and cannot be reopened.

Topology

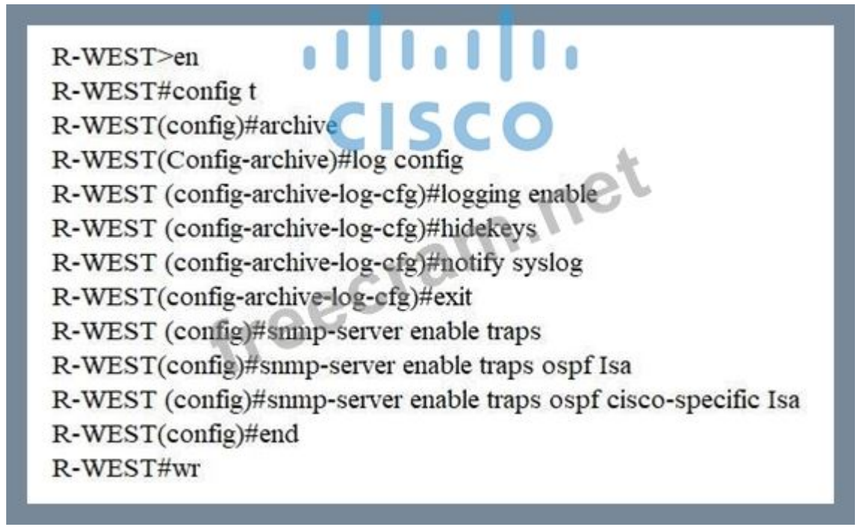



Tasks

Troubleshoot R-WEST to achieve the desired results:

1. All the commands should be locally saved to the router as well as sent to the Syslog server except passwords.
2. All the Cisco OSPF LSA traps should be sent to the SNMP server.

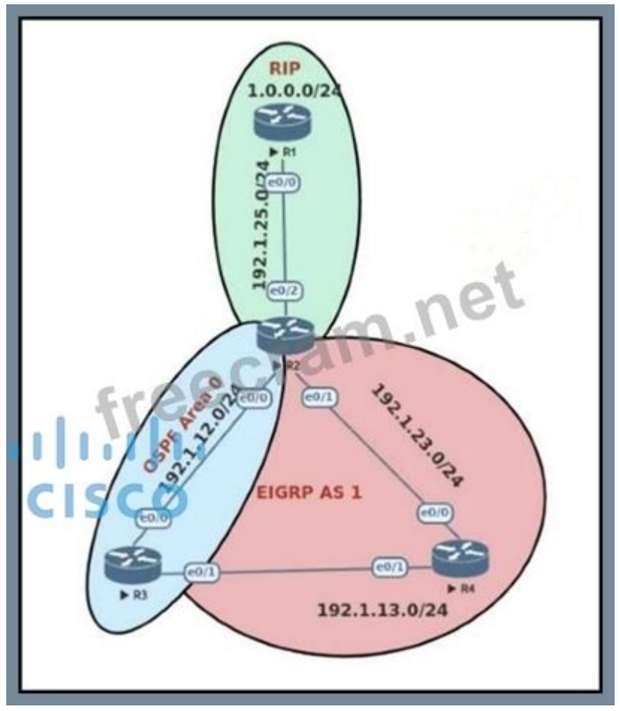
**Answer:**




**NEW QUESTION: 151**
When provisioning a device in Cisco Catalyst Center (formerly DNA Center), the engineer sees the error message "Cannot select the device. Not compatible with template.". What is the reason for the error?
**A.** The software version of the template is different from the software version of the device
**B.** The changes to the template were not committed
**C.** The template has an incorrect configuration.
**D.** The tag that was used to filter the templates does not match the device tag.
**Answer: (SHOW ANSWER)**
If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning: "Cannot select the device. Not compatible with template." Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network- automation-and-management/dna-center/1-2-10/user_guide/b_cisco_dna_center_ug_1_2_10/b_dnac_ug_1_2_10_chapter_0111.html

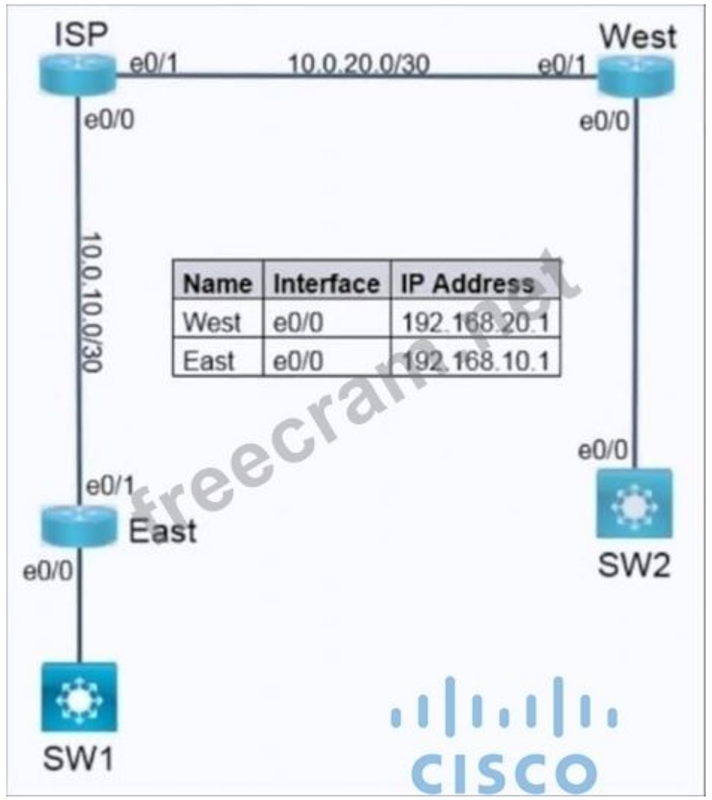


**NEW QUESTION: 152**
Refer to the exhibit. R3 is learning the 1.0.0.0/24 route through OSPF instead of EIGRP. Which action causes R3 to choose EIGRP to reach the 1.0.0.0/24 network?




**A.** Configure OSPF administrative distance to 120.
**B.** Configure EIGRP administrative distance to 110.
**C.** Configure OSPF administrative distance to 200.
**D.** Configure EIGRP administrative distance to 120.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 153**
LAB SIMULATION 14
Guidelines
This is a lab item in which tasks will be performed on virtual devices.
* Refer to the Tasks tab to view the tasks for this lab item.
* Refer to the Topology tab to access the device console(s) and perform the tasks.
* Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
* All necessary preconfigurations have been applied.
* Do not change the enable password or hostname for any device.
* Do not replace existing routing policies or configurations.
* Save your configurations to NVRAM before moving to the next item.
* Click Next at the bottom of the screen to submit this lab and move to the next question.
* When Next is clicked, the lab closes and cannot be reopened.
Topology




| Name | Interface | IP Address |
|---|---|---|
| West | e0/0 | 192.168.20.1 |
| East | e0/0 | 192.168.10.1 |



Tasks

Troubleshoot and resolve the issues on West and East routers to achieve these goals:

1. SW2 should only allow telnet access from ISP router's Loopback 0 using the AAA services. Fix the configs on SW2 to achieve this. Use preconfigured access-list ISP without removing the existing rule.

2. East router is configured to perform forwarding table lookup on an IP packet's source address, and it checks the incoming interface to reduce the risk of IP Address spoofing. Fix the issue where some East Router fails to ping destinations which are reachable via default route such as loopback 16 on ISP router. Do not advertise this interface into ospf and neither use a static route on East router to perform this task.

You must remove wrong  preconfigs that have impact on tasks you are performing to fix issues.

Enable password is 'Cisco' on all devices

SW2: Local username is "SW2" and password is "Cisco"

**Answer:**

Issue1:

To allow Telnet access on SW2 only for the ISP router's Loopback 0 address:

SW2 Configuration:

aaa new-model

aaa authentication login TELNET_AUTH local

line vty 0 4

login authentication TELNET_AUTH

transport input telnet

ip access-group ISP in

- The ISP access list ensures that only the ISP router's Loopback 0 address is permitted to access SW2 via Telnet.

- The aaa new-model and authentication login ensure proper AAA setup.
Issue 2:
To resolve the ping issue caused by strict uRPF on the East router:
East Router Configuration:
interface e0/0
ip verify unicast source reachable-via any
The reachable-via any command enables loose uRPF, allowing the router to verify the source address of incoming packets based on any route in the routing table.

**NEW QUESTION: 154**
Refer to the exhibit. A prefix list is created to filter routes inbound to an EIGRP process except for network 10 prefixes. After the prefix list is applied no network 10 prefixes are visible in the routing table from EIGRP.
Which configuration resolves the issue?

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

R1#show ip route eigrp
```

**A.** ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9.
**B.** ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
**C.** ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
**D.** ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
**Answer: (SHOW ANSWER)**
A prefix-list is an ordered list. "permit 10.0.0.0/8" needs to come before "deny 0.0.0.0/0 le 32" (deny everything), otherwise the "10" network is matched by the deny statement and thus, it gets to be filtered. "sequence 5" places the "permit 10.0.0.0/8" before "deny 0.0.0.0/0 le 32".
https://networklessons.com/eigrp/how-to-configure-prefix-list-on-cisco-router

**NEW QUESTION: 155**
Which of the following are control plane protocols used within a service provider MPLS network?
(Choose two.)
**A.** RSVP
**B.** SNMP
**C.** Targeted LDP
**D.** LDP
**E.** OAM
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 156**
Which of the following are used to validate the source of IPv6 traffic and are considered IPv6 layer 2 snooping features? (Choose two.)
**A.** DHCPv6 Root Guard

**B.** IPv6 Source Guard
**C.** IPv6 Prefix Guard
**D.** DHCPv6 Guard
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 157**
Refer to the exhibit. An engineer implemented an access list on R1 to allow anyone to Telnet except R2 Loopback0 to R1 Loopback4.
How must sequence 20 be replaced on the R1 access list to resolve the issue?

R1:

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

R2:

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



**A.** sequence 20 permit tcp host 1001:ABC:2011:7::1 host 400A:0:400C::1 eq telnet

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

**C.** sequence 20 permit tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet

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

**Answer: (SHOW ANSWER)**

This configuration example uses the ipv6 access-list access-list-name command in order to construct an IPv6 access list (named DENY_TELNET_Lo4) on router R1. A deny statement deny tcp host 400A:0:400C::1 host

1001:ABC:2011:7::1 eq telnet is followed by a permit statement permit ipv6 any any.

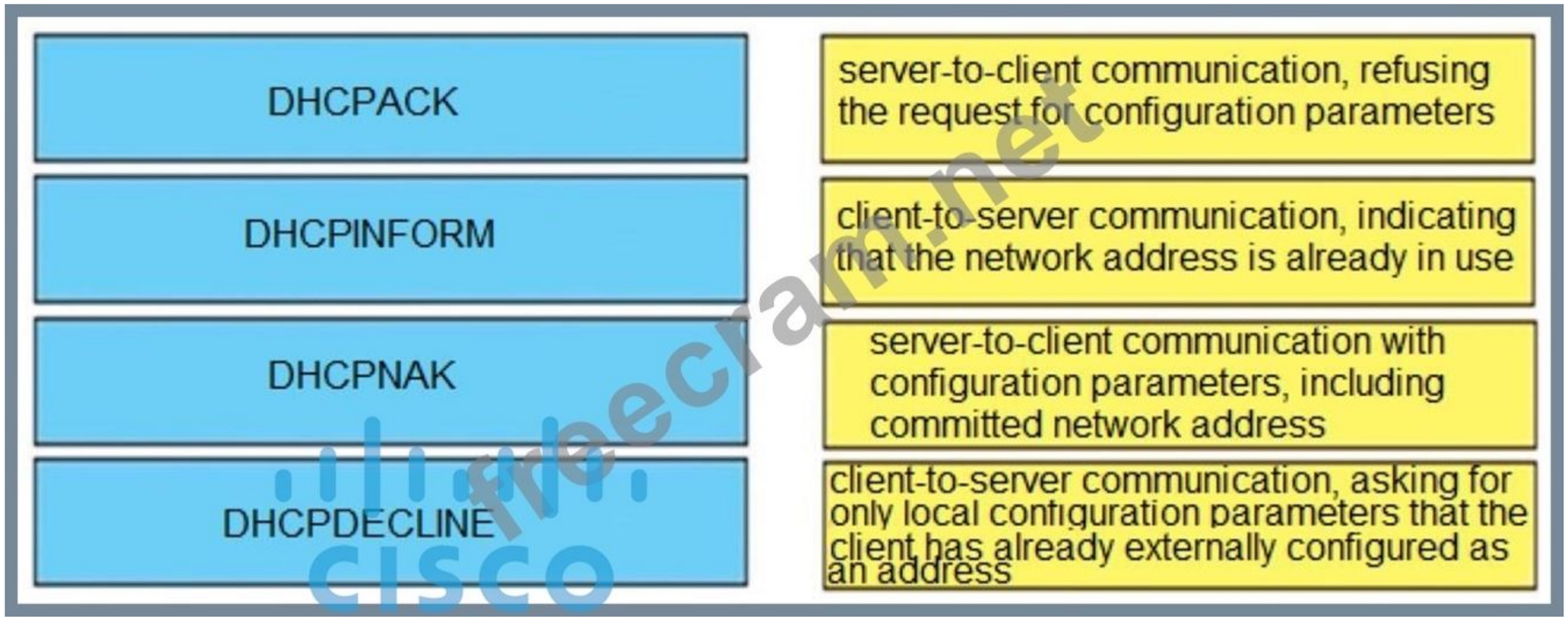
**NEW QUESTION: 158**
Refer to the exhibit. An engineer is trying to connect to a device with SSH but cannot connect.
The engineer connects by using the console and find the displayed output when troubleshooting.
Which command must be used in configuration mode to enable SSH on the device?

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

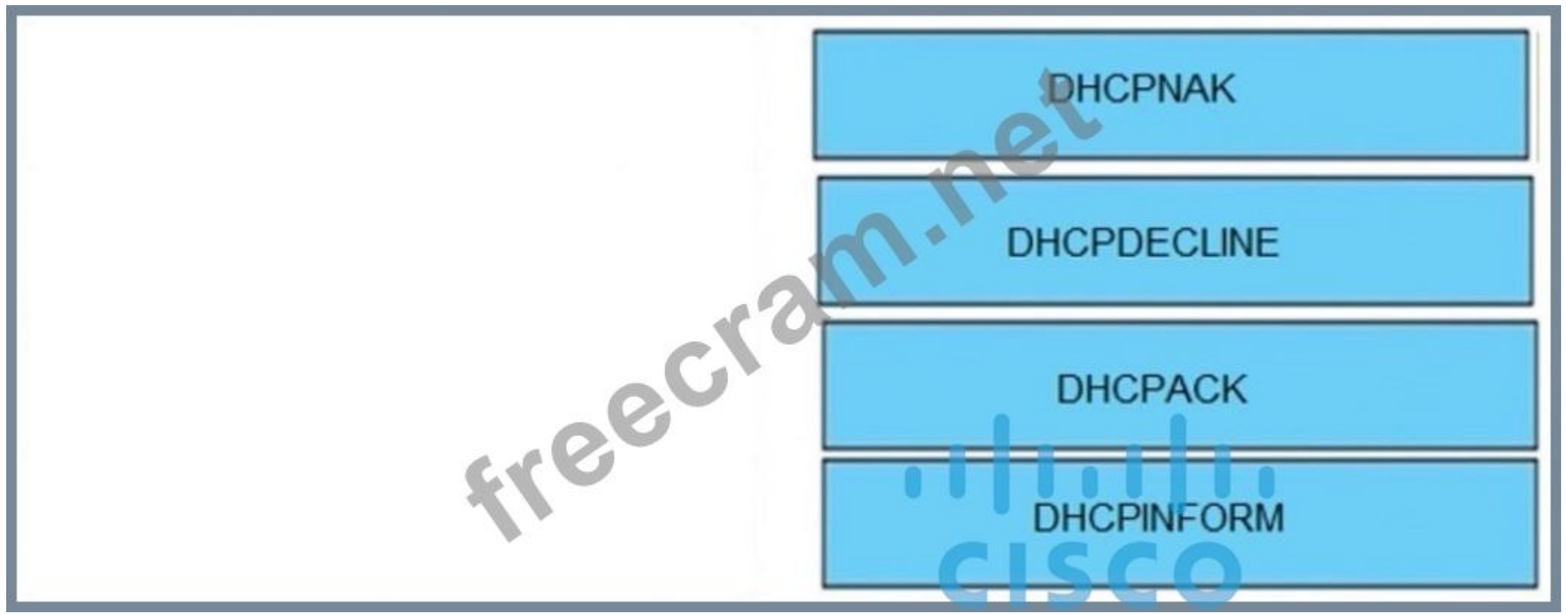


**A.** crypto key generate rsa
**B.** ip ssh enable
**C.** no ip ssh disable
**D.** ip ssh version 2
**Answer: (SHOW ANSWER)**
We see the notification "% Please create RSA keys to enable SSH" so we have to create RSA keys with the command:
R1(config)#crypto key generate rsa

**NEW QUESTION: 159**
Drag and Drop Question
Drag and drop the DHCP messages from the left onto the correct uses on the right.




**Answer:**




Explanation:

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: 160**

The network administrator configured CoPP so that EIGRP traffic toward the device is limited to 2 mbps. Any traffic that exceeds this limit must also be allowed at this point for traffic analysis.

```
access-list 100 permit EIGRP any any
!
class-map CM-EIGRP
match access-group 100
!
policy-map PM-COPP
class CM-EIGRP
police 2000000 conform-action transmit
!
control-plane
service-policy output PM-COPP
```

No EIGRP traffic is going through CoPP. Which configuration resolves the issue?

**A.** control-plane
no service-policy output PM-COPP
service-policy input PM-COPP

**B.** policy-map PM-COPP
class CM-EIGRP
police 2000000 conform-action transmit exceed-action transmit
!
control-plane
no service-policy output PM-COPP
service-policy input PM-COPP

**C.** policy-map PM-COPP
class CM-EIGRP
police 2000000 conform-action drop exceed-action drop
!
control-plane
no service-policy output PM-COPP
service-policy input PM-COPP

**D.** policy-map PM-COPP
class CM-EIGRP
police 2000000 conform-action transmit exceed-action transmit
**Answer: (SHOW ANSWER)**
Control Plane Policing (CoPP) policies should be applied in the input direction because they are meant to control traffic coming into the control plane (e.g., routing protocol traffic like EIGRP). The current configuration incorrectly applies the policy in the output direction, which doesn't affect inbound traffic.
To allow all EIGRP traffic (even if it exceeds the 2 Mbps rate) for analysis purposes, you need to set both conform-actionand exceed-actionto transmit. This ensures that no traffic is dropped, even above the threshold, but it still enforces rate monitoring.

**NEW QUESTION: 161**
How are packets forwarded in an MPLS domain?
**A.** Using a number that has been specified in a label
**B.** Using the MAC address of the frame
**C.** Using the destination IP address of the packet
**D.** Using the source IP address of the packet
**Answer: (SHOW ANSWER)**

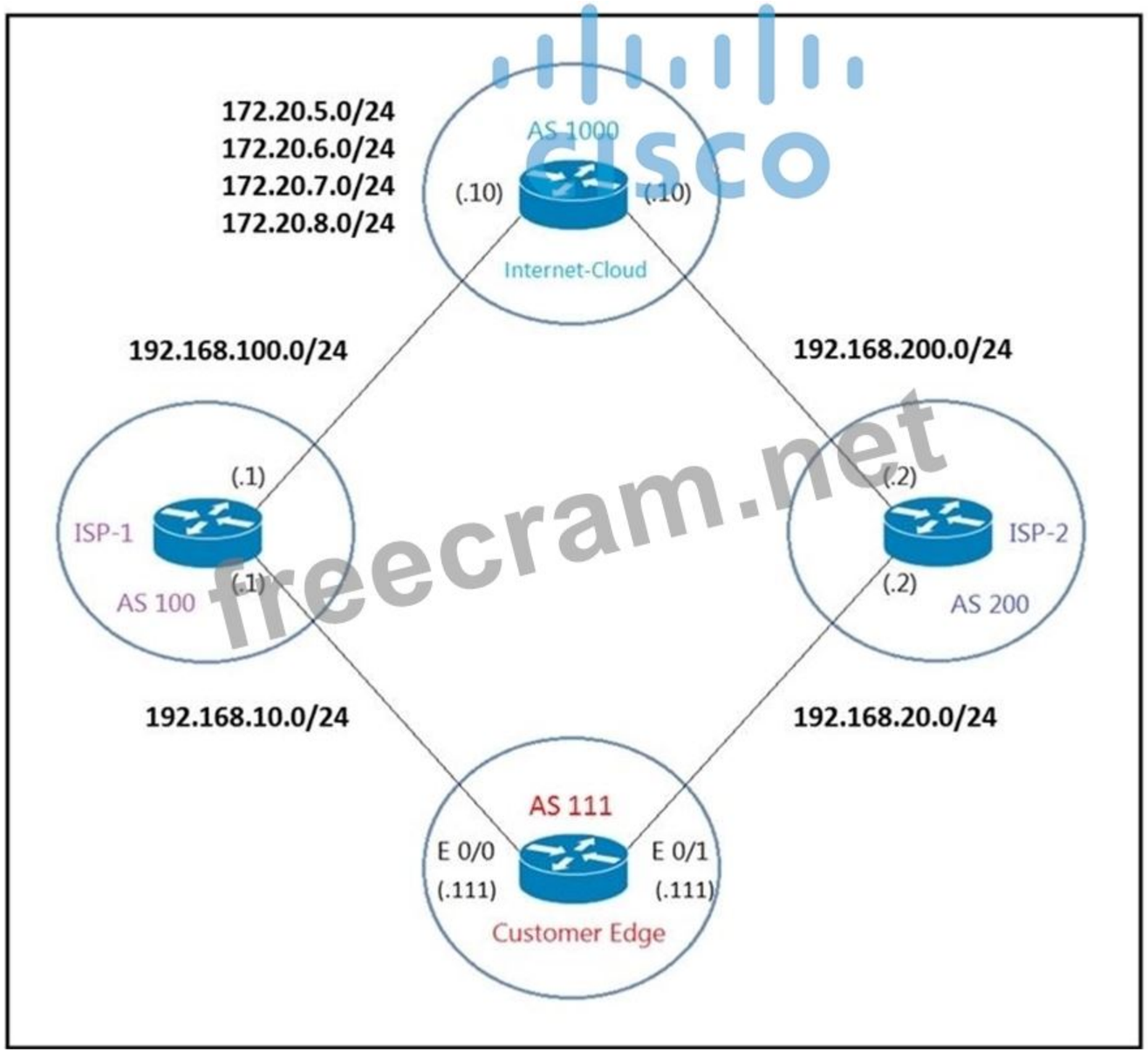
**NEW QUESTION: 162**
Refer to the exhibit. An engineer is trying to block the route to 192.168.2.2 from the routing table by using the configuration that is shown.
The route us still present in the routing table as an OSPF route. Which action blocks the route?

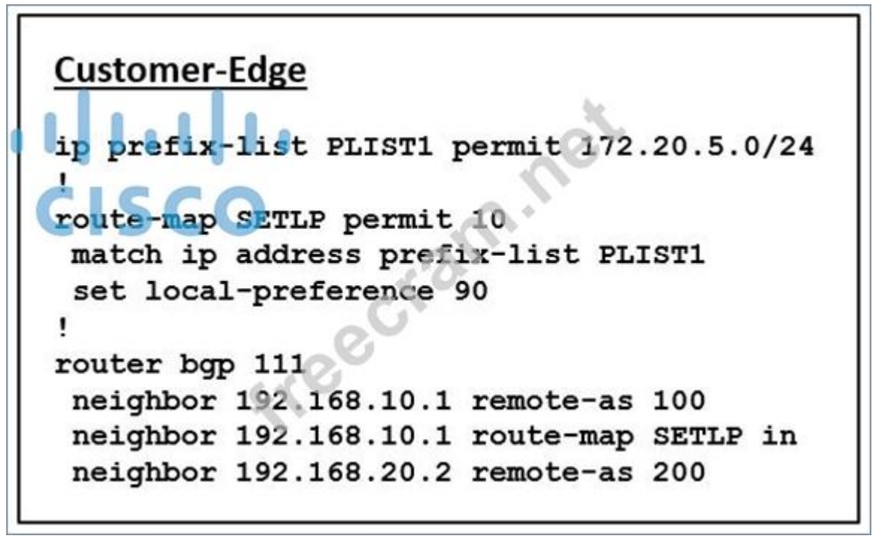
```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, permit, sequence 10
  Match clauses:
        ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#|
```



**A.** Add this statement to the route map route-map RM-OSPF-DL deny 20
**B.** Use a prefix list instead of an access list in the route map.
**C.** Change sequence 10 in the route-map command from permit to deny.
**D.** Use an extended access list instead of a standard access list.
**Answer: (SHOW ANSWER)**
To block a network or host prefix in a route-map the ACL format must be like this:
access-l 100 permit (or deny) host (ip address prefix) host (netmask) if you want to do this through acl if you use a prefix list is easier because the format is more compressible and intuitive to understand it.

**NEW QUESTION: 163**
Refer to Exhibit. AS 111 wanted to use AS 200 as the preferred path for 172.20.5.0/24 and AS 100 as the backup. After the configuration, AS 100 is not used for any other routes.
Whichconfiguration resolves the issue?

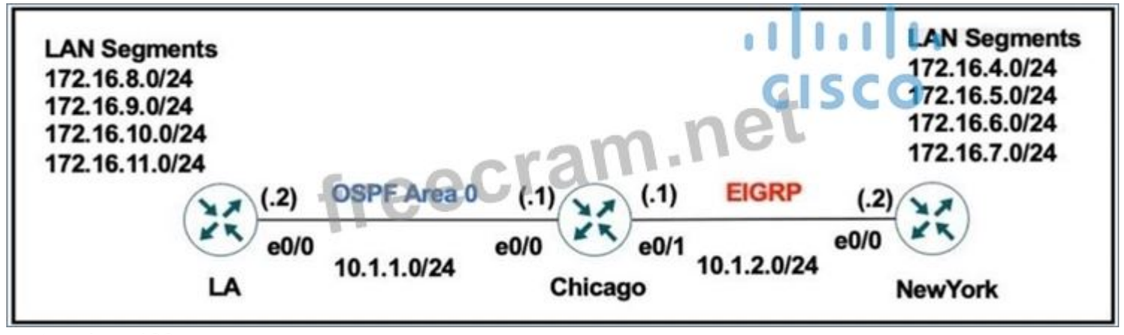





**A.** route-map SETLP permit 10
match ip address prefix-list PLIST1
set local-preference 110
route-map SETLP permit 20
**B.** route-map SETLP permit 10
match ip address prefix-list PLIST1
set local-preference 99
route-map SETLP permit 20
**C.** router bgp 111
no neighbor 192.168.10.1 route-map SETLP in
neighbor 192.168.20.2 route-map SETLP in
**D.** router bgp 111
no neighbor 192.169.10.1 route-map SETLP in
neighbor 192.168.10.1 route-map SETLP out
**Answer: (SHOW ANSWER)**
There is an implicit deny all at the end of any route-map so all other traffic that does not match
172.20.5.0/24 would be dropped. Therefore we have to add a permitsequence at the end of the route-map to allow other traffic.
The default value of Local Preference is 100 and higher value is preferred so we have to set the local preference of AS100 lower than that of AS200.

**NEW QUESTION: 164**
Which failure detection mechanism is used for BFD?
**A.** variable rate
**B.** Layer 2 protocol failure
**C.** routing protocol failure
**D.** consistent rate
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 165**
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:

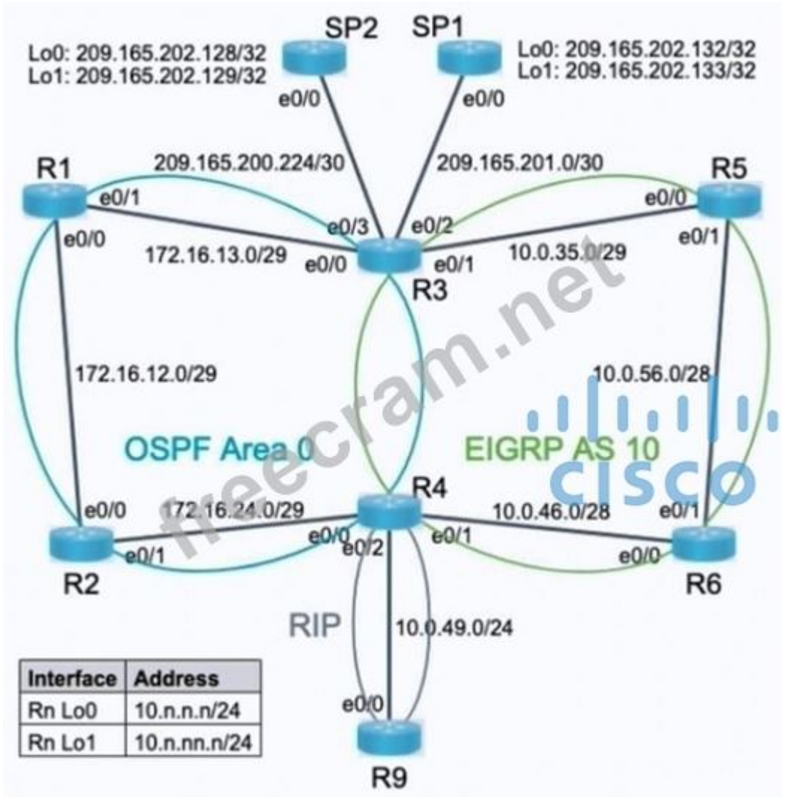



router eigrp 100
redistribute ospf 1 metric 10 10 10 10 10
router ospf 1 redistribute eigrp 100 subnets
!
interface E 0/0
ip summary-address eigrp 100 172.16.0.0 255.255.0.0
After the configuration, the New York router receives all the specific LA routes but the summary route.
Which set of configurations resolves the issue on the Chicago router?
**A.** interface E 0/1
ip summary-address eigrp 100 172.16.0.0 255.255.0.0
**B.** interface E 0/1
ip summary-address eigrp 100 172.16.8.0 255.255.252.0
**C.** router eigrp 100
summary-address 172.16.8.0 255.255.252.0
**D.** router eigrp 100
summary-address 172.16.0.0 255.255.0.0
**Answer: (SHOW ANSWER)**
Rather than advertise out each individual network you can just advertise a summary route
192.168.1.0 225.255.252.0 using the "ip summary-address eigrp" command. You would configure this under the interface configuration on the access-layer switch that connects to the distribution switch.

**NEW QUESTION: 166**
LAB SIMULATION 16
Guidelines
This is a lab item in which tasks will be performed on virtual devices.
* Refer to the Tasks tab to view the tasks for this lab item.
* Refer to the Topology tab to access the device console(s) and perform the tasks.
* Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
* Do not change the enable password or hostname for any device.
* All necessary preconfigurations have been applied.
* Do not replace existing routing policies or configurations.

* Save your configurations to NVRAM before moving to the next item.
* Click Next at the bottom of the screen to submit this lab and move to the next question.
* When Next is clicked, the lab closes and cannot be reopened.

Topology




Tasks

Troubleshoot and resolve the issues to achieve these goals:

1. Ensure that R5 can ping the prefix 10.9.99.9. Manipulate the first basic routing decision-making criteria that if a router learns a route from different routing protocols the admin distance can be changed without using a route-map. Use decimal value of 85 if required to accomplish this.

2. Ensure that R5 loopback 0 reaches to R2's loopback 0 by following the path through R5, R6, R4 to R2 and vice versa. Use metric values K1= 100000, K2=1, K3=255, K4=10, K5=1500 to modify the default metric in EIGRP if required. Do not add or modify the default-metric command under router eigrp 10. Do not use a route-map.

3. Ensure that on R3, prefix 10.0.0.0/8 uses the SP2 to route to the Internet, whereas prefix
172.16.0.0/12 uses the SP1 to route to the Internet. Do not use BGP to accomplish this. Use the pre-configured route-maps SP1 and SP2 and modify to accomplish the task if required. Use the ping and trace commands from R5 and R1 to verify results.

**Answer:**

Task 1:

1. On R4, modify the administrative distance for RIP so that EIGRP routes are preferred.

router rip

distance 85

2. Verify:

- Check the routing table of R5 and ensure the prefix 10.9.99.9 is being learned through R4.
- Use ping 10.9.99.9 from R5.

Task 2:

1. Modify EIGRP metrics on R6 and R4 to ensure this path is preferred. Apply the following metrics:

interface e0/0

metric weights 0 100000 1 255 10 1500

2. Verify:
- On R5, check the EIGRP topology table (show ip eigrp topology) to confirm the preferred path.
- Use trace 10.2.2.2 (R2's loopback 0) from R5 to confirm the traffic path.

Task 3:

Prefix 10.0.0.0/8 uses SP2.

Prefix 172.16.0.0/12 uses SP1.

1. Modify the pre-configured route maps on R3.

For SP2:

route-map SP2 permit 10

match ip address 10

set ip next-hop 209.165.202.128

For SP1:

route-map SP1 permit 10

match ip address 172

set ip next-hop 209.165.201.1

2. Verify:
- Use trace and ping commands from R1 and R5 to confirm the paths for 10.0.0.0/8 and 172.16.0.0/12.
- Confirm the correct route maps are applied on the relevant interfaces.



**NEW QUESTION: 167**

In a typical MPLS VPN, which routers act as the MPLS label imposition and disposition points in the network?

**A.** P router

**B.** Core router

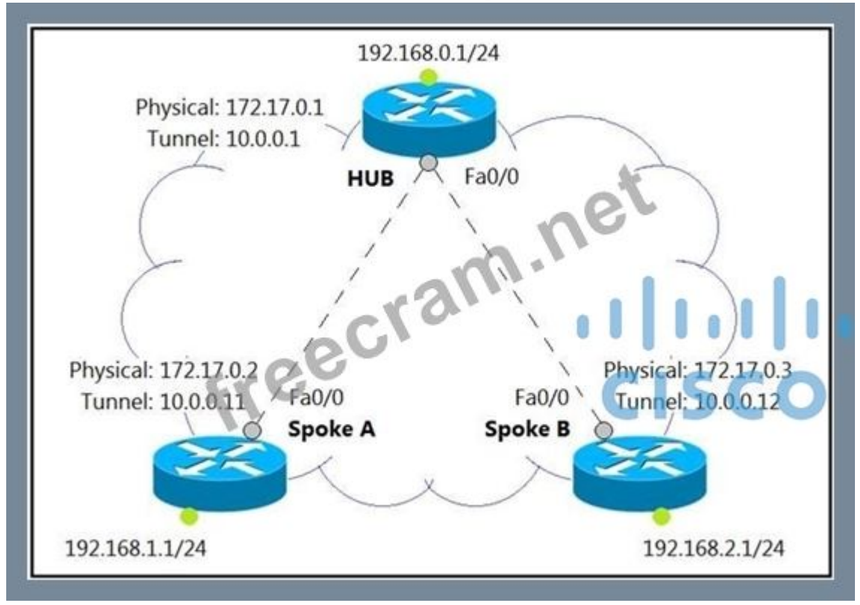
**C.** CE Router

**D.** PE Router

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 168**

Refer to the exhibit. An administrator is setting up above shown routers to enable MVPN with mGRE mode. What would be the recommended interface configuration that must be done by the engineer to make it to work?




**A.** interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel destination 172.17.0.2
tunnel mode IPsec multipoint

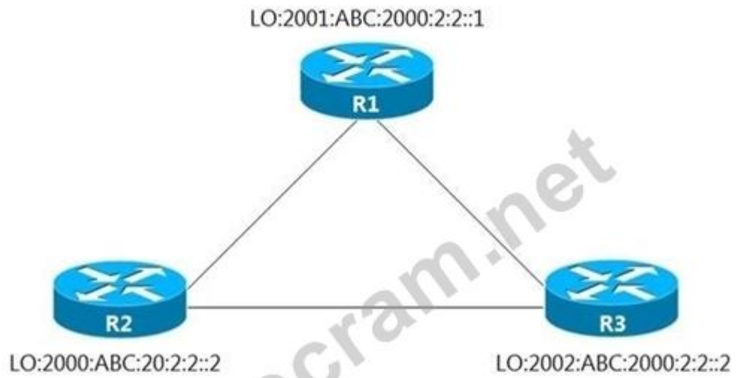
**B.** interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode IPSec multipoint

**C.** interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0
ip nhrp network-id 1
tunnel source 172.17.0.1
tunnel mode IPsec multipoint

**D.** interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0

ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint
**Answer: (SHOW ANSWER)**

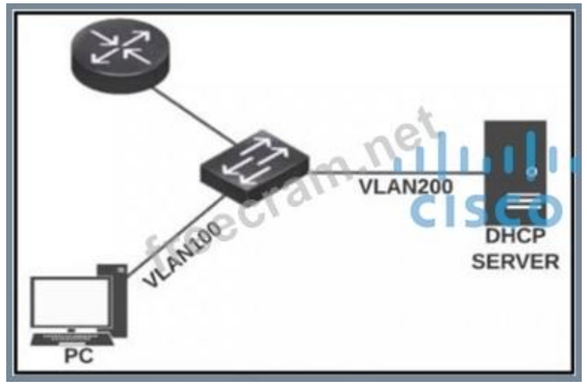
**NEW QUESTION: 169**
Refer to the exhibit. An IPv6 network was newly deployed in the environment and the help desk reports that R3 cannot SSH to the R2s Loopback interface. Which action resolves the issue?




```
IPv6 access list PERMIT_SSH
10 deny tcp 2001:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
20 permit tcp 2001:ABC:2000:2:2::/64 host 2000:ABC:20:2:2::2 eq 22
30 deny tcp 2002:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
40 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
50 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
60 permit tcp host 2002:ABC:2000:2:2::2 host 2000:ABC:20:2:2::2 eq 22
70 deny ipv6 any any
```

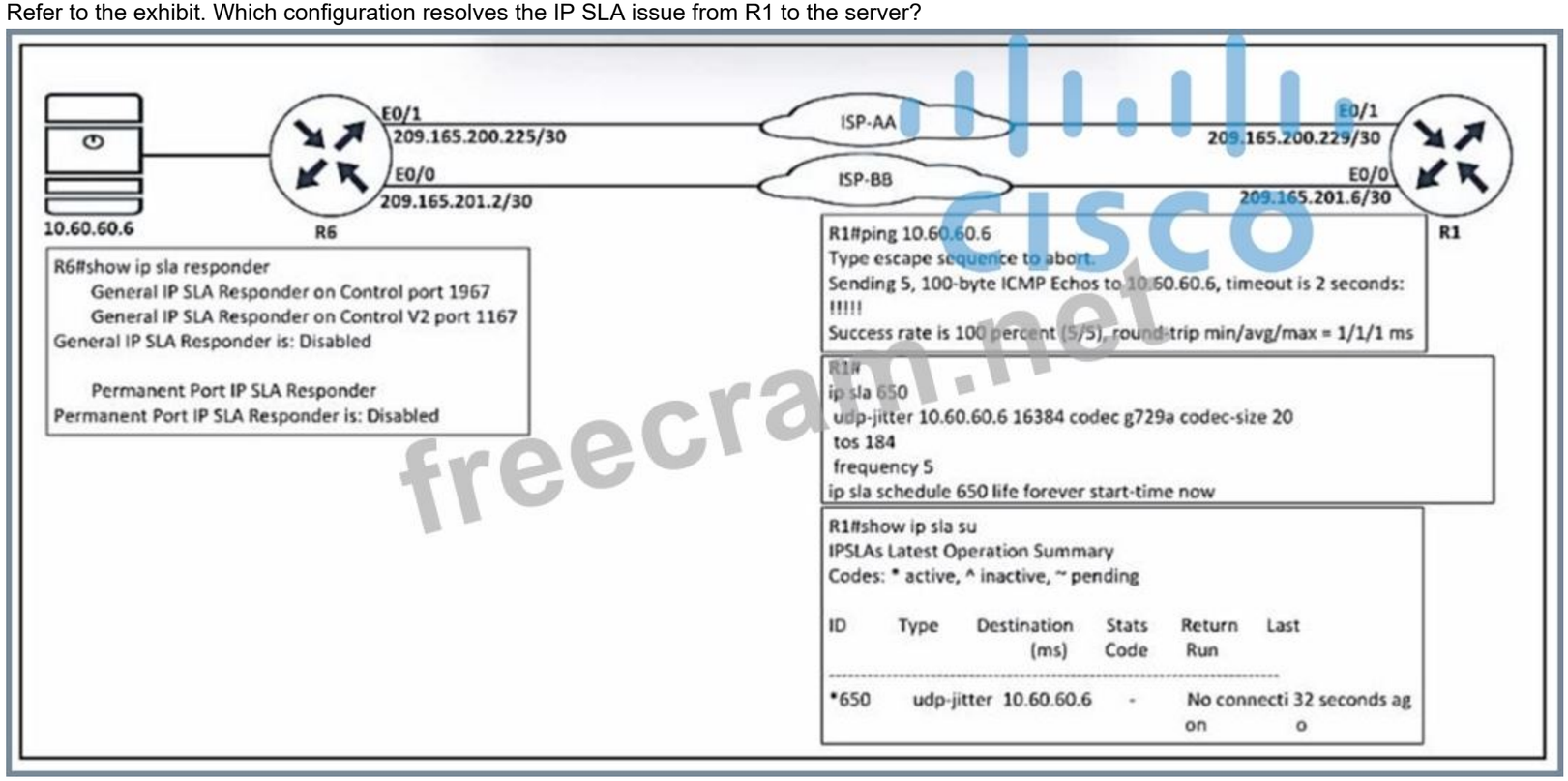
**A.** Modify line 10 of the access list to permit instead of deny
**B.** Remove line 60 from the access list.
**C.** Modify line 30 of the access list to permit instead of deny.
**D.** Remove line 70 from the access list.
**Answer: (SHOW ANSWER)**
The SSH traffic from R3 matches the broader deny entry for the 2002:ABC:2000::/36 source range before it reaches the more specific permit entry for R3's loopback address. Changing that deny entry to permit allows the SSH session to R2's loopback interface.

**NEW QUESTION: 170**
Refer to the exhibit. A PC is configured to obtain an IP address automatically, but it receives an IP address only from the 169.254.0.0 subnet. The DHCP server logs contained no DHCPDISCOVER message from the MAC address of the PC. Which action resolves the issue?




**A.** Configure a static IP address on the PC and exclude it from the DHCP pool.
**B.** Configure DHCP Snooping on the switch to forward DHCP messages to the server.
**C.** Configure an ip helper-address on the router to forward DHCP messages to the server.
**D.** Configure a DHCP reservation on the server for the PC.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 171**
Refer to the exhibit. Which configuration resolves the IP SLA issue from R1 to the server?

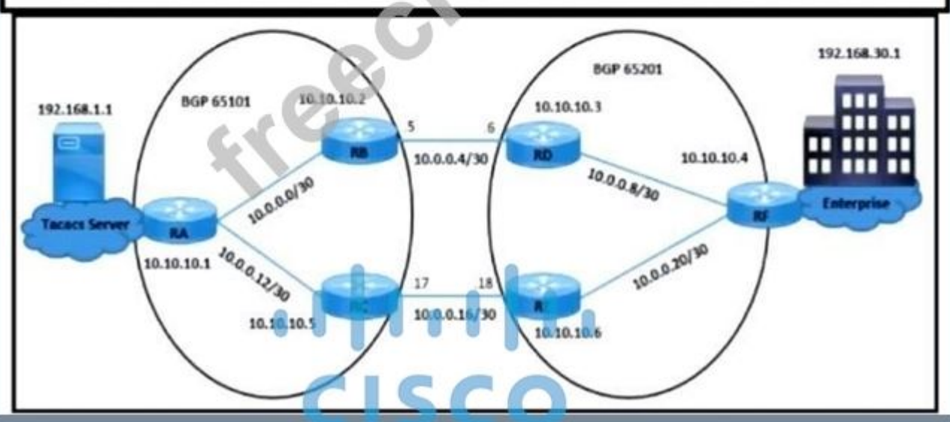



**A.** R6(config)#ip sla 650

R6(config-ip-sla)#udp-jitter 10.60.60.6
**B.** R6(config)#ip sla responder
**C.** R6(config)#ip sla responder
udp-echo ipaddress 10.60.60.6 po 5000
**D.** R6(config)#ip sla schedule 10 life forever start-time now
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 172**
Refer to the exhibit. The enterprise users fail to authenticate with the TACACS server when a direct fiber link fails between RB and RD. The NOC team observes:
- Users connected on AS65201 fail to authenticate with TACACS server
192.168.1.1
- Users connected on AS65101 successfully authenticate with TACACS
server 192.168.1.1
- All AS65101 and AS65201 users are configured to authenticate with the TACACS server Which configuration resolves the issue?

```
RF#traceroute 192.168.1.1
  1 10.0.0.9 40 msec 28 msec 24 msec
  2  *  *  *
  3  *  *  *
RE#show  ip prefix-list detail
Prefix-list with the last deletion/insertion: Customer
ip prefix-list Customer:
   count: 2, range entries: 1, sequences: 5 - 10, refcount: 3
   seq 5 deny 192.168.1.1/32 (hit count: 5, refcount: 1)
   seq 10 permit 0.0.0.0/0 le 32 (hit count: 26, refcount: 1)

RC#show  ip prefix-list detail
Prefix-list with the last deletion/insertion: Customer
ip prefix-list Customer:
   count: 1, range entries: 1, sequences: 10 - 10, refcount: 4
   seq 10 permit 0.0.0.0/0 le 32 (hit count: 7, refcount: 1)
```



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

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

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

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

**Answer: (SHOW ANSWER)**

The issue arises because the prefix-list on router RF explicitly denies the route to the TACACS server (192.168.1.1/32). This configuration prevents the TACACS server's route from being propagated to AS 65201, causing authentication failures for users in AS 65201 when the direct link between RB and RD fails.

The prefix-list denying 192.168.1.1/32 on RF must be removed. This will allow the route to the TACACS server to propagate correctly across the BGP network, ensuring that AS 65201 users can authenticate even when the direct link is down.

**NEW QUESTION: 173**

What does IPv6 Source Guard utilize to determine if IPv6 source addresses should be forwarded?

**A.** ACE

**B.** ACLS

**C.** DHCP

**D.** Binding Table

**Answer: (SHOW ANSWER)**

IPv6 Source Guard filters inbound traffic on L2 switch ports that are not in the IPv6 binding table.

The binding table stores the following information:

+ IPv6 address
+ MAC address
+ VLAN
+ Interface ID

Source Guard only looks at information found in the binding table, and it doesn't fill the binding table.

**NEW QUESTION: 174**

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

**A.** DMVPN

**B.** MPLS VPN

**C.** Virtual Tunnel Interface (VTI)

**D.** SSL VPN

**E.** PPPoE

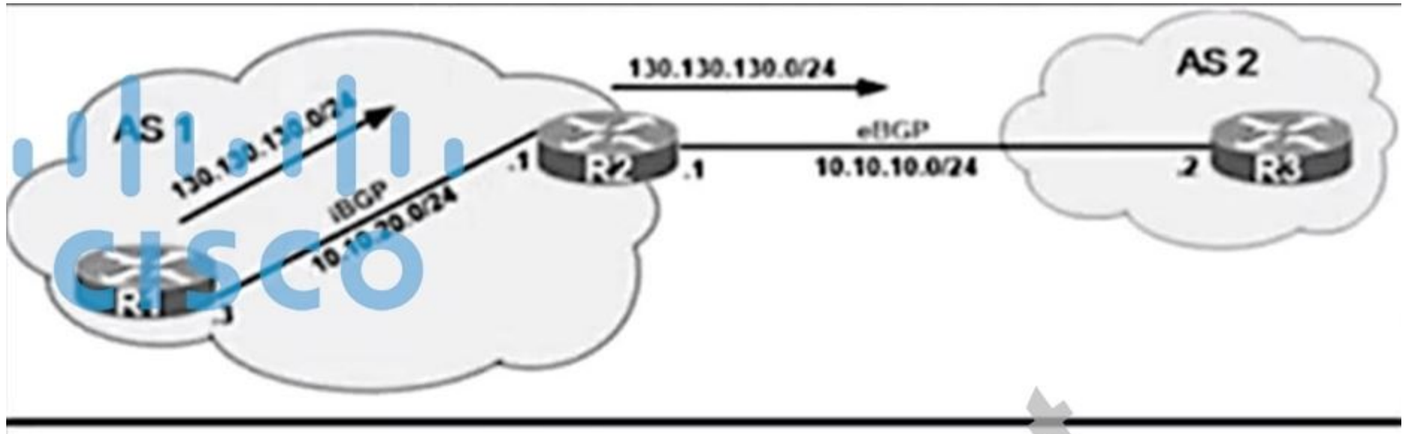
**Answer: (SHOW ANSWER)**

IP security (IPsec) virtual tunnel interfaces (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network.

IPsec VTIs simplify configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.

**NEW QUESTION: 175**

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?




**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

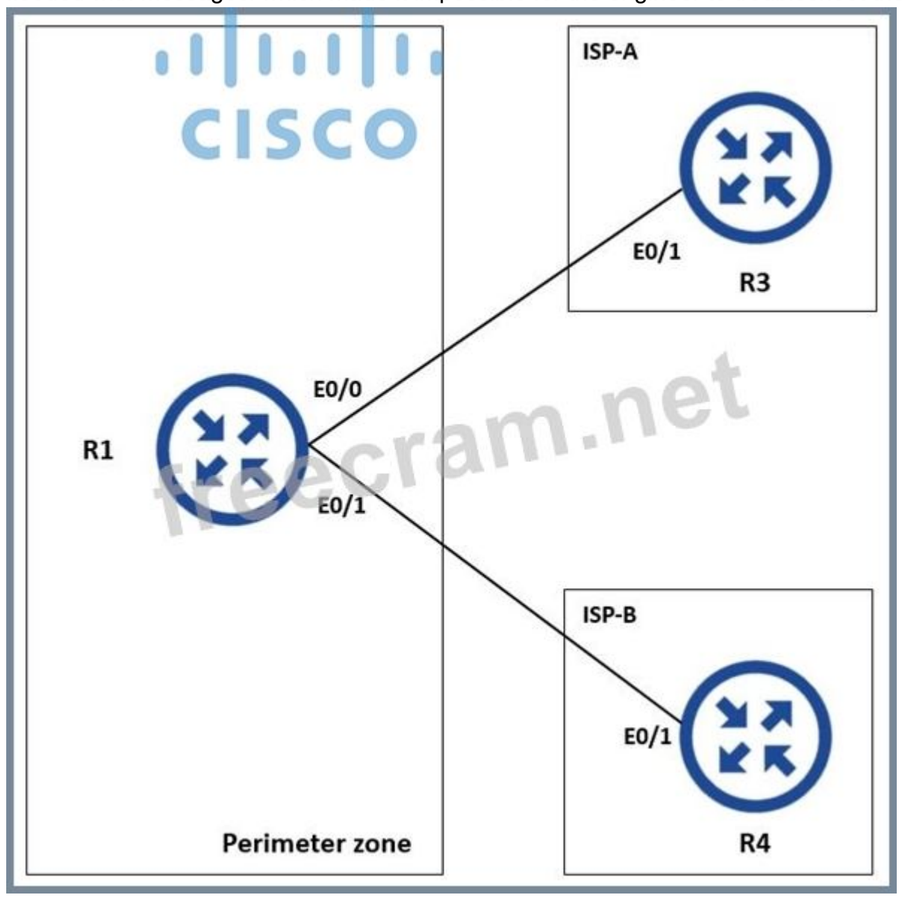
| Network | Next Hop | Metric | LocPrf | Weight | Path |
|---|---|---|---|---|---|
| * i130.130.130.0/24 | 10.10.20.3 | 0 | 100 | 0 | i |

**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

**A.** Automatic route summarization must be enabled on R2.
**B.** The outgoing filter list for all interfaces must be set on R2.

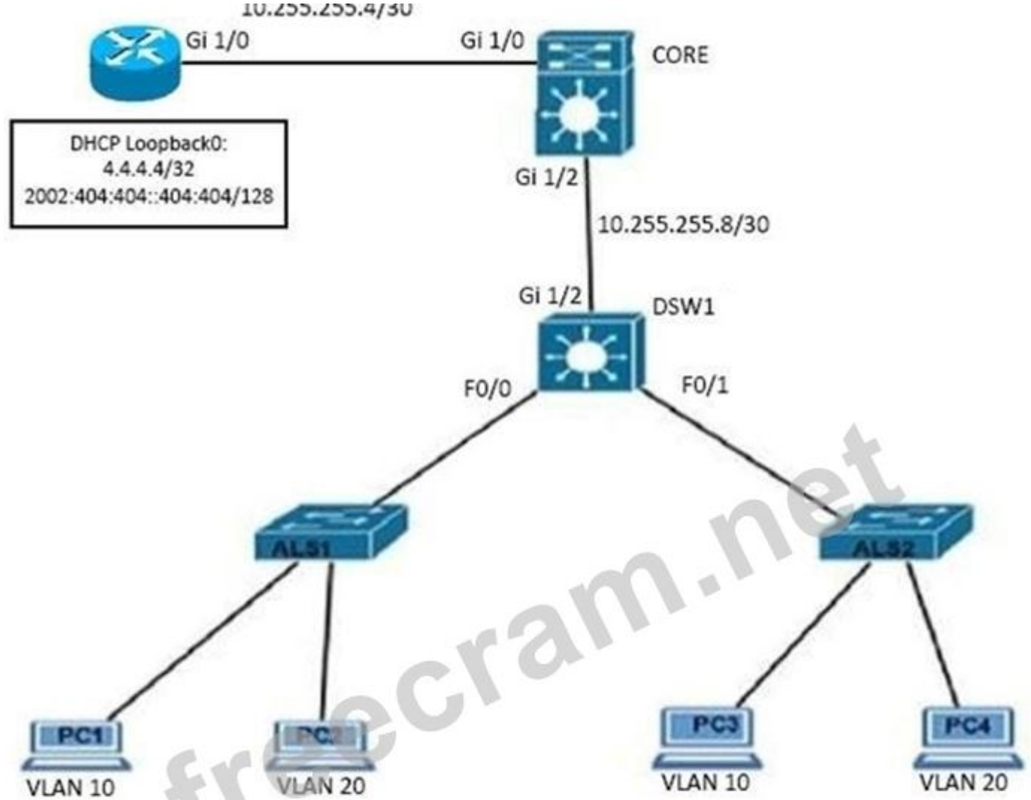
**C.** The incoming filter list for all interfaces must be set on R2.
**D.** IGP synchronization must be disabled on R2.
**Answer: (SHOW ANSWER)**
The exhibit shows that BGP synchronization is enabled on R2, as indicated in the output of show ip protocols. BGP synchronization requires that a route must also exist in the IGP (such as OSPF or EIGRP) before BGP can advertise it to its peers. Since the route 130.130.130.0/24 is in the BGP table but likely not in the IGP routing table, R2 does not advertise the route to R3.
To resolve this, disabling BGP synchronization on R2 allows BGP to advertise the route to R3 without requiring it to be present in the IGP.

**NEW QUESTION: 176**
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 messagesi which made it impossible for the engineer to troubleshoot the issue. Which command resolves this issue on R1?




**A.** (config)#terminai no monitor
**B.** #terminal no monitor
**C.** no terminal monitor
**D.** (config)#no terminal monitor
**Answer: (SHOW ANSWER)**
**NEW QUESTION: 177**

Refer to the exhibit. Router DHCP is configured to lease IPv4 and IPv6 addresses to clients on ALS1 and ALS2. Clients on ALS2 receive IPv4 and IPv6 addresses. Clients on ALS1 receive IPv4 addresses. Which configuration on DSW1 allows clients on ALS1 to receive IPv6 addresses?




```
DSW1#sh run int f0/0
Building configuration...

Current configuration : 174 bytes
!
interface FastEthernet 0/0
 ip address 10.4.10.1 255.255.255.0
 ip helper-address 4.4.4.4
 duplex auto
 speed auto
 ipv6 address 2002:A04:A01::A04:A01/120
 ipv6 enable
end
```

**A.** DSW1(config-if)# ipv6 helper address 2002:404:404::404:404

**B.** DSW1(config)#ipv6 route 2002:404:404::404:404/128 FastEthernet 1/0

**C.** DSW1(dhcp-config)# default-router 2002:A04:A01::A04:A01

**D.** DSW1(config)# ipv6 dhcp relay destination 2002:404:404::404:404 GigabitEthernet 1/2

**Answer: D (LEAVE A REPLY)**
Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.
Enable the IPv6 DHCP relay agent function and specifies the IPv6 address as a destination address to which the client messages are forwarded.

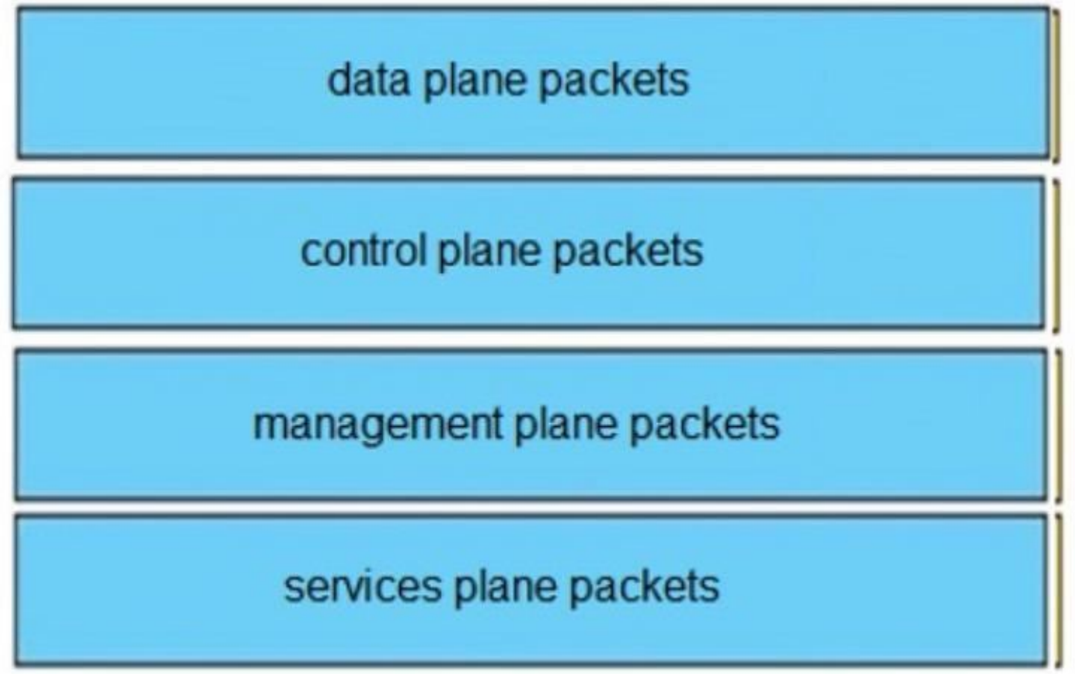
**NEW QUESTION: 178**
Which protocol is used in a DMVPN network to map logical IP address to physical IP addresses?
**A.** BGP
**B.** LLDP
**C.** EIGRP
**D.** NHRP
**Answer: (SHOW ANSWER)**
Next Hop Resolution Protocol (NHRP), defined in RFC 2332, is a Layer 2 address resolution protocol and cache, like Address Resolution Protocol (ARP). NHRP is used by a branch router connected to a non-broadcast, multi-access (NBMA) sub-network to determine the IP address of the "NBMA next hop"; in this case, the headend router or the destination IP address of another branch router.
NHRP is used to map tunnel IP addresses to "physical" or "real" IP addresses, used by endpoint routers. It resolves private addresses (those behind mGRE and optionally IPSEC) to a public address. NHRP is layer 2 resolution protocol and cache, much like Address Resolution Protocol (ARP) or Reverse ARP (Frame Relay).

**NEW QUESTION: 179**
Drag and Drop Question
Drag and drop the packet types from the left onto the correct descriptions on the right.

| | |
|---|---|
| data plane packets | user-generated packets that are always forwarded by network devices to other end-station devices |
| control plane packets | network device generated or received packets that are used for the creation of the network itself |
| management plane packets | network device generated or received packets; packets that are used to operate the network |
| services plane packets | user-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than the normal traffic by the network devices |

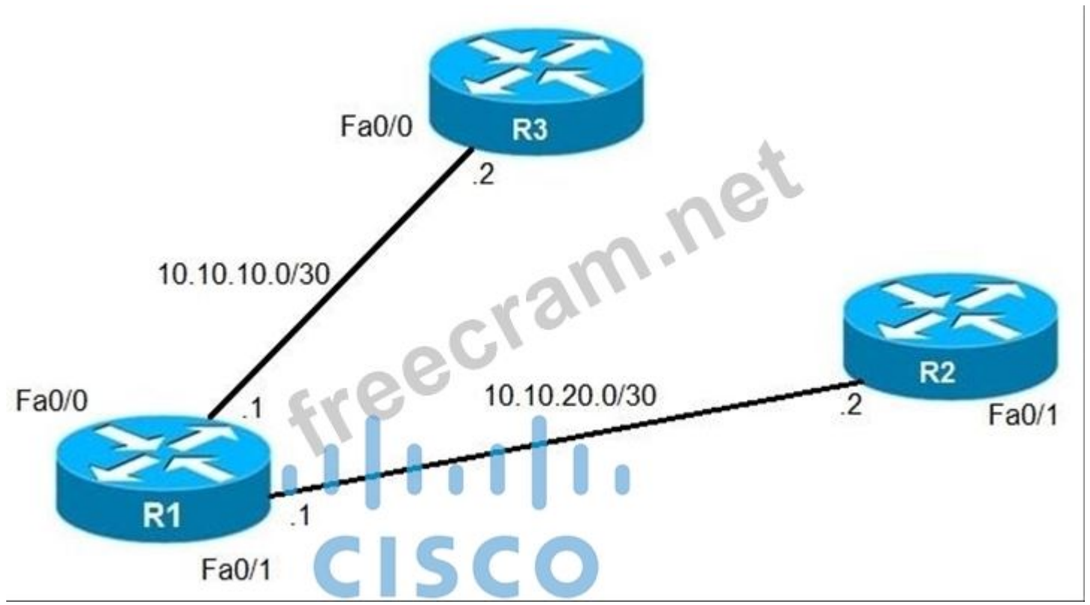


**Answer:**




Explanation:
Unlike legacy network technologies such as ISDN, Frame Relay, and ATM that defined separate data and control channels, IP carries all packets within a single pipe. Thus, IP network devices such as routers and switches must be able to distinguish between data plane, control plane, and management plane packets to treat each packet appropriately.
From an IP traffic plane perspective, packets may be divided into four distinct, logical groups:
1. Data plane packets - End-station, user-generated packets that are always forwarded by network devices to other end-station devices. From the perspective of the network device, data plane packets always have a transit destination IP address and can be handled by normal, destination IP address-based forwarding processes.
2. Control plane packets - Network device generated or received packets that are used for the creation and operation of the network itself. From the perspective of the network device, control plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor. Examples include protocols such as ARP, BGP, OSPF, and other protocols that glue the network together.
3. Management plane packets - Network device generated or received packets, or management station generated or received packets that are used to manage the network. From the perspective of the network device, management plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor. Examples include protocols such as Telnet, Secure Shell (SSH), TFTP, SNMP, FTP, NTP, and other protocols used to manage the device and/or network.
4. Services plane packets - A special case of data plane packets, services plane packets are also user-generated packets that are also forwarded by network devices to other end-station devices, but that require high-touch handling by the network device (above and beyond normal, destination IP address-based forwarding) to forward the packet. Examples of high-touch handling include such functions as GRE encapsulation, QoS, MPLS VPNs, and SSL/IPsec encryption/decryption, etc. From the perspective of the network device, services plane packets may have a transit destination IP address, or may have a receive destination IP address (for example, in the case of a VPN tunnel endpoint).
Reference: https://tools.cisco.com/security/center/resources/copp_best_practices

**NEW QUESTION: 180**
Refer to the exhibit. An IP SLA was configured on router R1 that allows the default route to be modified in the event that Fa0/0 losses reachability with the router R3 Fa0/0 interface.
The route has changed to flow through route R2.
Which debug command is used to troubleshoot this issue?




**A.** debug ip flow
**B.** debug ip sla error
**C.** debug ip routing
**D.** debug ip packet
**Answer: (SHOW ANSWER)**
The "debug ip routing" command enables debugging messages related to the routing table. Since the routing table is normally stable, you will only see debug messages when there are any changes in the routing table.

**NEW QUESTION: 181**
What is a characteristic of IPv6 RA Guard?
**A.** It is supported on the egress direction of the switch
**B.** RA messages are allowed from the host port to the switch
**C.** It filters rogue RA broadcasts from connected hosts
**D.** It is unable to protect tunneled traffic
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 182**
A network administrator notices that the BGP state drops and logs are generated for missing BGP hello keepalives. What is the potential problem?
**A.** Incorrect neighbor options
**B.** Hello timer mismatch

**C.** BGP path MTU enabled
**D.** MTU mismatch
**Answer: (SHOW ANSWER)**
BGP neighbors form; however, at the time of prefix exchange, the BGP state drops and the logs generate missing BGP hello keepalives or the other peer terminates the session.
Here are some possible causes:
*The interface MTU on both routers do not match.
*The interface MTU on both routers match, but the Layer 2 domain over which the BGP session is formed does not match.
*Path MTU discovery determined the incorrect max datasize for the TCP BGP session.
*The BGP Path Maximum Transmission Unit Discovery (PMTUD) could be failing due to PMTUD ICMP packets blocked (firewal or ACL)
http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/116377-troubleshoot- bgp-mtu.html

**NEW QUESTION: 183**
Which IP SLA operation can be used to simulate voice traffic on a network?
**A.** TCP connect
**B.** UDP-jitter
**C.** ICMP-echo
**D.** ICMP-jitter
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 184**
Refer to the exhibit. 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?

```
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
```



**A.** The redistributed prefixes should be advertised as Type 1.
**B.** The administrative distance should be raised to 120 from the ASBR 10.4.17.6.
**C.** The ASBR 10.4.17.6 should assign a tag to match and assign a lower metric on R1.
**D.** The administrative distance should be raised to 120 from the ASBR 10.4.15.5.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 185**
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
```

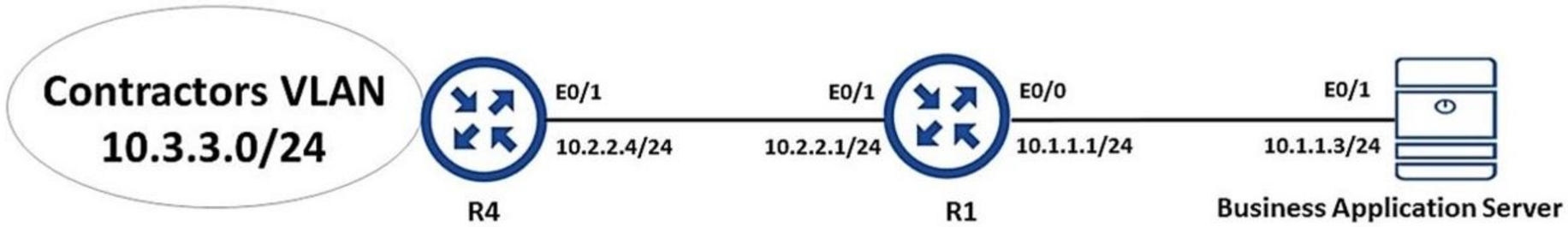
**D.**
```
ip as-path access-list 1 permit ^$
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

**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: 186**
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?




```
R4#ping 10.1.1.3
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
```

```
R1#
interface Ethernet0/10
  ip address 10.1.1.1 255.255.255.0
  ip access-group 101 out
!
time-range Contractor
periodic weekdays 8:00 to 16:30
!
End
R1#show ip access-lists
Extended IP access list 101
    10 permit tcp 10.2.2.0 0.0.0.255 host 10.1.1.3 eq telnet time-range
Contractor (inactive)
    20 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range
Contractor (inactive)
    30 permit tcp 10.2.2.0 0.0.0.255 host 10.1.1.3 eq www time-range
Contractor (inactive)
    40 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq www time-range
Contractor (inactive)
    50 permit icmp any any (30 matches)
    60 permit ospf any any (92 matches)
```

```
R4#show access-list
Extended IP access list 101
    10 permit tcp 10.2.2.2.0 0.0.0.255 host 10.1.1.3 eq telnet time-range
Contractor (inactive)
    20 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range
Contractor (inactive)
    30 permit tcp 10.2.2.0 0.0.0.255 host 10.1.1.3 eq www time-range Contractor
(inactive)
    40 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq www time-range Contractor
(inactive)
    50 permit icmp any any
    60 permit ospf any any
```

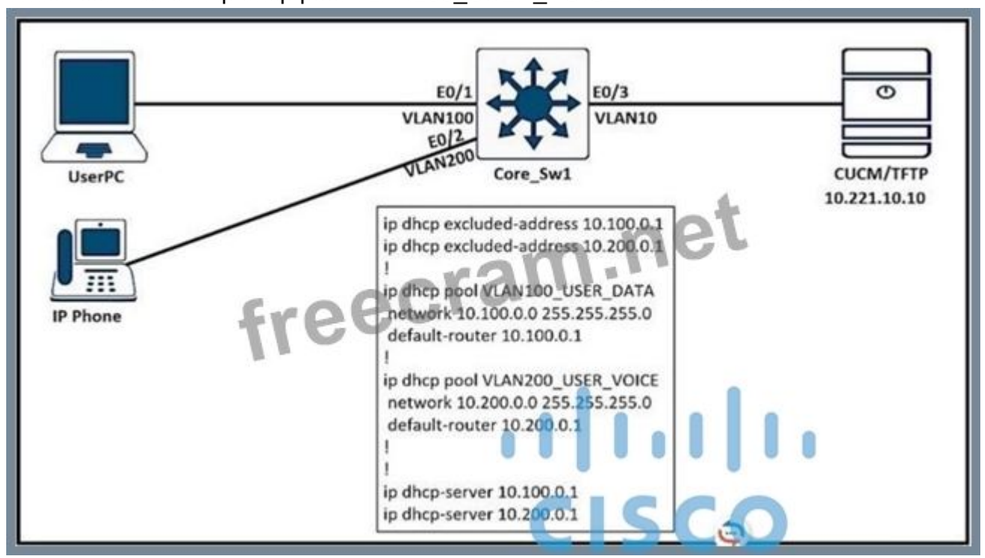


**A.** R4
no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor
**B.** R1
time-range Contractor
no periodic weekdays 8:00 to 16:30
periodic daily 8:00 to 16:30
**C.** R1
no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor
**D.** R4
time-range Contractor
no periodic weekdays 17:00 to 23:59
periodic daily 8:00 to 16:30
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 187**

Refer to the exhibit. UserPC receives the IP address but does not register to the call manager.

Which command in ip dhcp pool VLAN200_USER_VOICE resolves the issue?




**A.** option 15 ip 10.221.10.10

**B.** option 160 ip 10.221.10.10

**C.** option 150 ip 10.221.10.10

**D.** option 117 ip 10.221.10.10

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 188**

What is an advantage of implementing BFD?

**A.** BFD provides millisecond failure detection

**B.** BFD provides better capabilities to maintain the routing table

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

**D.** BFD provides faster updates for any flapping route.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 189**

Which router attaches the VPN label to incoming packets from CE routing?

**A.** core router

**B.** PE router

**C.** CE router

**D.** P router

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 190**

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



**A.** Create link dampening on links to protect the session.
**B.** Increase input queue on links to protect the session.
**C.** Create targeted hellos to protect the session.
**D.** Increase a hold-timer to protect the session.
**E.** Increase a session delay to protect the session.
**Answer: (SHOW ANSWER)**
To avoid having to rebuild the LDP session altogether, you can protect it. When the LDP session between two directly connected LSRs is protected, a targeted LDP session is built between the two LSRs. When the directly connected link does go down between the two LSRs, the targeted LDP session is kept up as long as an alternative path exists between the two LSRs. For the protection to work, you need to enable it on both the LSRs. If this is not possible, you can enable it on one LSR, and the other LSR can accept the targeted LDP Hellos by configuring the command mpls ldp discovery targeted-hello accept.
Reference:
https://www.ccexpert.us/mpls-network/mpls-ldp-session-protection.html
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECMPL-3201.pdf Troubleshooting LDP Issues Problem:
I. When a link flaps (for a short time),
...
Solution:
+ When LDP session supported by link hello is setup, create a targeted hello to protect the session.

**NEW QUESTION: 191**
Refer to the exhibit. R1 uses SP1 as the primary path. A network engineer must force all SSH traffic generated from R1 toward SP2. Which configuration accomplishes the task?


A.
```
p access-list extended match_SSH
permit tcp any any eq 22

oute-map PBR_SSH permit 10
match ip address match_SSH
set ip next-hop 10.20.20.1

nterface Gig0/0
ip policy route-map PBR_SSH
```

B.
```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.10.10.1
!
ip local policy route-map PBR_SSH
```

C.
```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
ip local policy route-map PBR_SSH
```
D.
```
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
interface Gig0/1
 ip policy route-map PBR_SSH
```

**Answer: (SHOW ANSWER)**

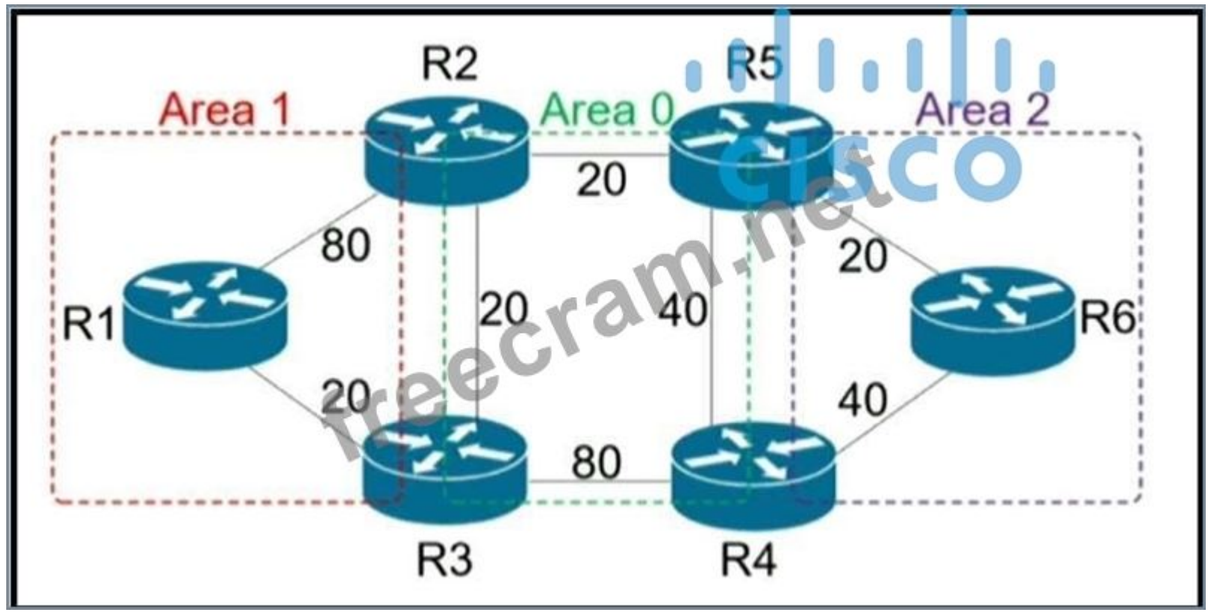
To direct SSH traffic originating from the router (R1) to use a specific next-hop (SP2 in this case), you must use local policy-based routing (PBR). Local PBR allows you to apply a route-map to locally generated traffic (traffic initiated by R1 itself).

- Access Control List (ACL) matches the locally generated SSH traffic (permit tcp any any eq 22).
- Route Map specifies the action for the matched traffic (setting the next-hop to SP2, 10.20.20.1).
- Local Policy applies the route map to the router's locally generated traffic using ip local policy route-map.

This configuration ensures that all SSH traffic generated from R1 is sent to SP2, overriding the default routing behavior.

**NEW QUESTION: 192**

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

**Answer: (SHOW ANSWER)**

Traditional IP routing emphasizes on forwarding traffic to the destination as fast as possible. As a result, the routing protocols find out the least-cost route according to its metric to each destination in the network and every router forwards the packet based on the destination IP address and packets are forwarded hop-by-hop. Thus, traditional IP routing does not consider the available bandwidth of the link. This can cause some links to be over-utilized compared to others and bandwidth is not efficiently utilized. Traffic Engineering (TE) is used when the problems result from inefficient mapping of traffic streams onto the network resources. Traffic engineering allows you to control the path that data packets follow and moves traffic flows from congested links to non-congested links that would not be possible by the automatically computed destination-based shortest path.

**NEW QUESTION: 193**

A company Is redesigning WAN infrastructure so that all branch sites must communicate via the head office and the head office can directly communicate with each site independently. The network engineer must configure the head office router by considering zero-touch technology when adding new sites in the same WAN infrastructure.
Which configuration must be applied to the head office router to meet this requirement?

```
interface Tunnel0
 tunnel mode ip
 ip nhrp map multicast dynamic
```

```
interface Tunnel0
 tunnel mode dvmrp
 ip nhrp redirect
```

```
interface Tunnel0
 tunnel mode ip
 ip nhrp redirect
```

```
interface Tunnel0
 tunnel mode gre multipoint
 ip nhrp map multicast dynamic
```

**A.** Option B

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

**NEW QUESTION: 194**
Refer to the exhibit. Which configuration enables OSPF for area 0 interfaces to establish adjacency with a neighboring router with the same VRF?


**A.** router ospf 1 vrf CCNP
network 10.0.0.0 0.0.255.255 area 0
**B.** router ospf 1
interface Ethernet1
ip ospf 1 area 0.0.0.0
interface Ethernet2
ip ospf 1 area 0.0.0.0
**C.** router ospf 1 vrf CCNP
network 10.1.1.1 0.0.0.0 area 0
network 10.2.2.2 0.0.0.0 area 0
**D.** router ospf 1 vrf CCNP
interface Ethernet1
ip ospf 1 area 0.0.0.0
interface Ethernet2
ip ospf 1 area 0.0.0.0
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 195**
Refer to the exhibit. Two routers are connected back to back via Gigabit Ethernet 0/0 interfaces.
Which configuration provides VRF-Lite connectivity for two separate VRFs using the prefixes 10.1.1.0/24 for one VRF and 10.2.2.0/24 for the other VRF?

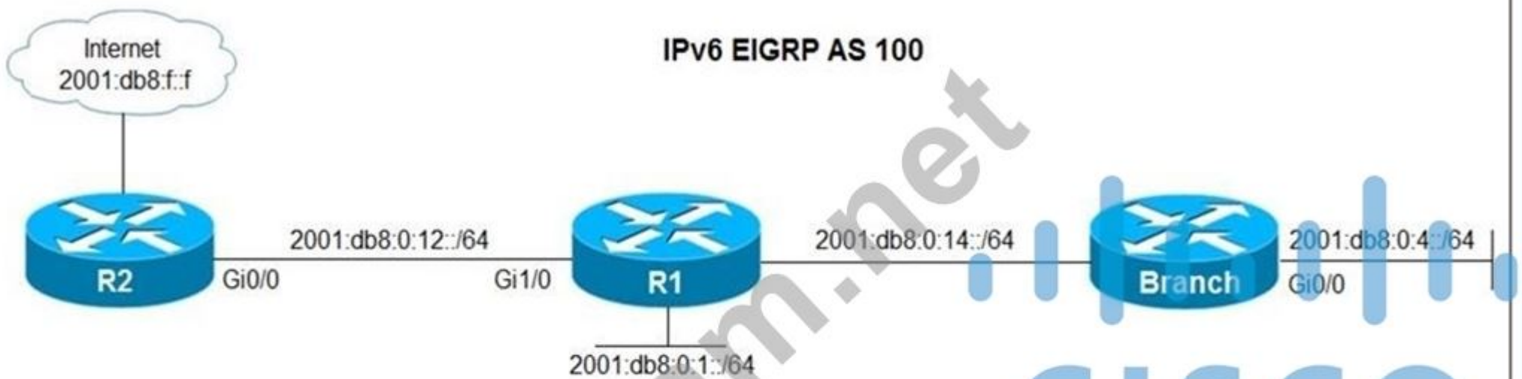
```
int GigabitEthernet0/0
  no shut
int GigabitEthernet0/0.1
  encapsulation dot1Q 1
  ip address 10.1.1.1 255.255.255.0
int GigabitEthernet0/0.2
  encapsulation dot1Q 2
  ip address 10.2.2.1 255.255.255.0
```



**A.** ip vrf 1
ip vrf 2
int GigabitEthernet0/0
no shut
!
int GigabitEthernet0/0.1
encapsulation dot1Q 1
ip vrf forwarding 1
ip address 10.1.1.1 255.255.255.0
!
int GigabitEthernet0/0.2
encapsulation dot1Q 2
ip vrf forwarding 2
ip address 10.2.2.1 255.255.255.0
**B.** ip vrf 1
rd 65001:1
ip vrf 2
rd 65001:2
!
int GigabitEthernet0/0
no shut
!
int GigabitEthernet0/0.1
encapsulation dot1Q 1
ip vrf forwarding
ip address 10.1.1.1 255.255.255.0
!
int GigabitEthernet0/0.2
encapsulation dot1Q 2
ip vrf forwarding
ip address 10.2.2.1 255.255.255.0
**C.** ip vrf 1

ip vrf 2
!
int GigabitEthernet0/0
no shut
!
int GigabitEthernet0/0.1
encapsulation dot1Q 1
ip address 10.1.1.1 255.255.255.0
ip vrf forwarding 1
!
int GigabitEthernet0/0.2
encapsulation dot1Q 2
ip address 10.2.2.1 255.255.255.0
ip vrf forwarding 2
**D.** ip vrf 1
rd 65001:1
ip vrf 2
rd 65001:1
!
int GigabitEthernet0/0
no shut
!
int GigabitEthernet0/0.1
encapsulation dot1Q 1
ip vrf forwarding 1
ip address 10.1.1.1 255.255.255.0
!
int GigabitEthernet0/0.2
encapsulation dot1Q 2
ip vrf forwarding 2
ip address 10.2.2.1 255.255.255.0
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 196**
Refer to the exhibit. Users in the branch network of 2001:db8:0:4::/64 report that they cannot access the Internet. Which command is issued in IPv6 router EIGRP 100 configuration mode to solve this issue?




```
R1# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(100)/ID(10.1.12.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 28416
        via FE80::C828:DFF:FEF4:1C (28416/2816), FastEthernet3/0
P 2001:DB8:0:1::/64, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P ::/0, 1 successors, FD is 2816
        via FE80::C821:17FF:FE04:8 (2816/256), GigabitEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
        via Connected, FastEthernet3/0
P 2001:DB8:0:12::/64, 1 successors, FD is 2816
        via Connected, GigabitEthernet1/0
```

```
Branch# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(100)/ID(4.4.4.4)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P 2001:DB8:0:1::/64, 1 successors, FD is 28416
        via FE80::C820:17FF:FE04:54 (28416/2816), FastEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
        via Connected, FastEthernet1/0
P 2001:DB8:0:12::/64, 1 successors, FD is 28416
        via FE80::C820:17FF:FE04:54 (28416/2816), FastEthernet1/0
```

**A.** Issue the eigrp stub command on R1.
**B.** Issue the no eigrp stub command on R1.
**C.** Issue the eigrp stub command on R2.
**D.** Issue the no eigrp stub command on R2.
**Answer: (SHOW ANSWER)**
In the output of R1, we see R1 has a default route to the Internet via G1/0, which is correct but R2 does not have this route. One reasonable answer of this issue is R1 has been configured as a stub router so it only advertised connected and summary routes. In Branch router output, we also see routes that are directly connected to R1 only.
Note: In this topology, only Branch router should be configured as stub, not R1 router.



**NEW QUESTION: 197**

You have configured policy-based routing on router R1 to force some traffic to go over an alternate link. In order to verify the configuration, which debug command should be used to verify that the specific traffic is taking the intended path?

**A.** Debug policy map

**B.** Debug ip policy

**C.** Debug ip routing

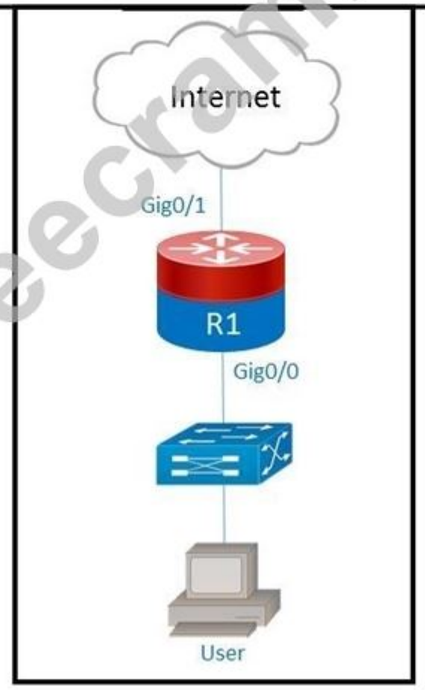
**D.** Debug policy routing

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 198**

Refer to the exhibit. Users on a call center report that they cannot browse the internet on Saturdays during the afternoon. Which configuration resolves the issue?

```
R1#show time-range

time-range entry: timer (active)
   periodic weekend 9:00 to 17:00
   used in: IP ACL entry
   used in: IP ACL entry

R1#show ip access-list interface gig0/0

Extended IP access list NO_Internet in
   10 deny tcp any any eq www time-range timer (active)
   20 deny tcp any any eq 443 time-range timer (active)
   30 permit ip any any
```

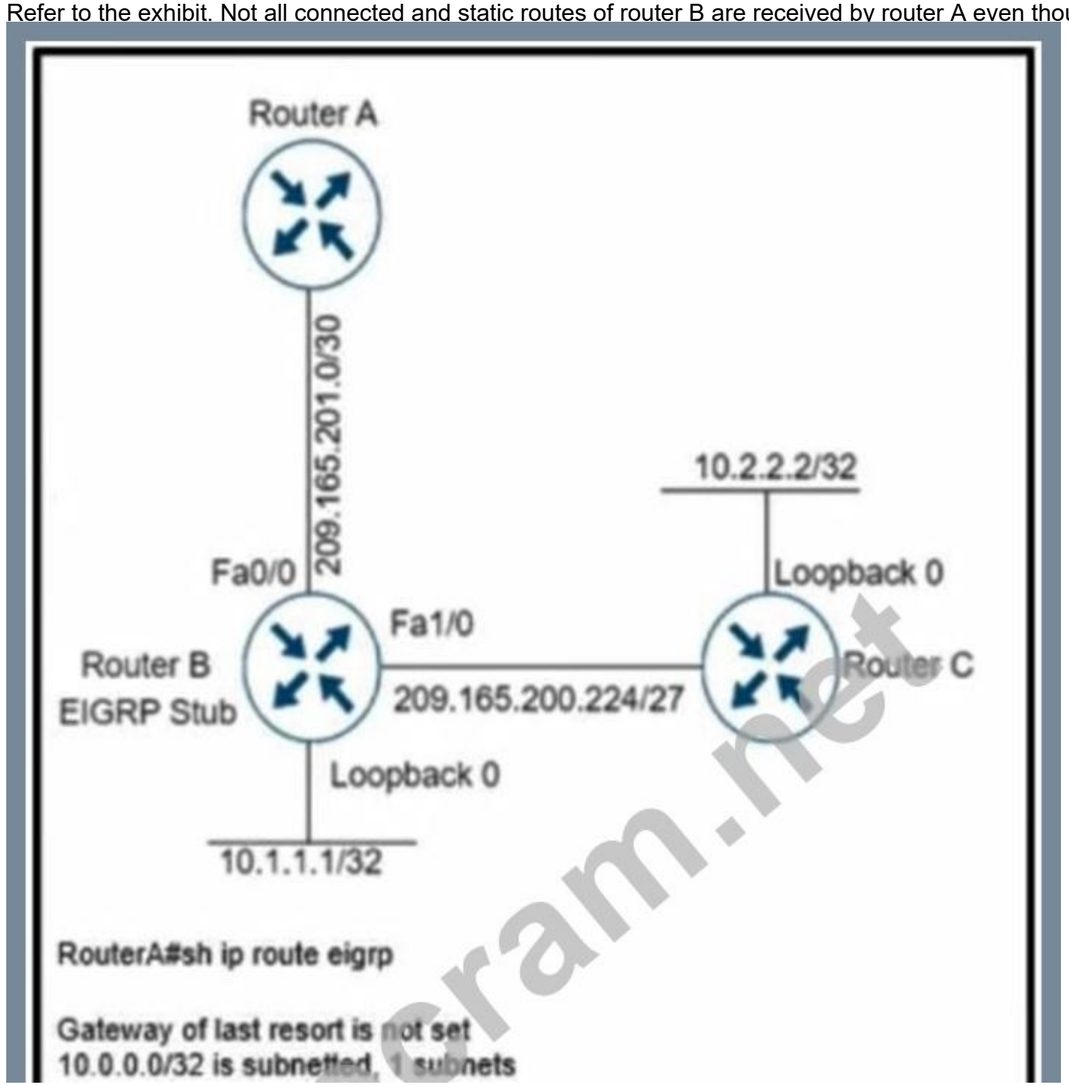


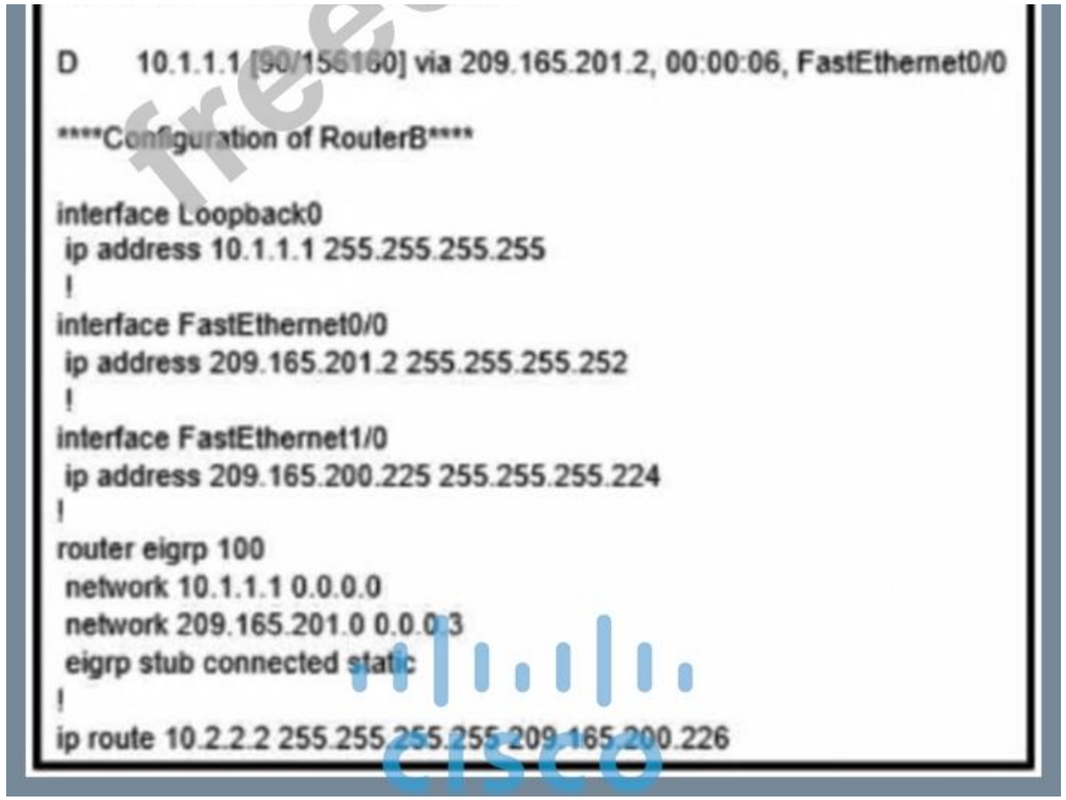

**A.** ip access-list extended NO_Internet
15 permit tcp any any eq www
**B.** interface gig0/0
ip access-group NO_Internet out
**C.** no time-range timer
**D.** time-range timer
no periodic weekend 9:00 to 17:00
periodic weekend 17:00 to 23:59

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 199**
What must be configured by the network engineer to circumvent AS_PATH loop prevention mechanism in IP/VPN Hub and Spoke deployment scenarios?
**A.** Use Allowas-in the PE_Hub
**B.** Use allows in and as-override at all Pes.
**C.** Use allowas in and as-override at the PE-Hub.
**D.** Use as-override at the PE_Hub
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 200**
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: C (LEAVE A REPLY)**
Router B is configured as an EIGRP stub with connectedand staticas the only types of routes it can advertise. However, currently it only has eigrp stub connected static configured, but static routes are not being redistributed. To advertise the static route to
10.2.2.2/32 to Router A, Router B must redistribute static routes with a defined EIGRP metric and ensure that the stub type allows static routes (which eigrp stub staticdoes).
Also, the networkcommand must include the interface connected to Router C (209.165.200.224/27), and 0.0.0.7correctly matches the subnet (usable range from .225 to .230 for a /27 subnet).

**NEW QUESTION: 201**
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?

```
R1#show bgp ipv6 unicast 2001:db8::1/128
BGP routing table entry for 2001:db8::1/128, version 3
Paths: (1 available, best #1, table Global-IPv6-Table)
  Not advertised to any peer
  Local
    2001:db8:33:33::33 (metric 128) from 2001:db8:11:11::11 (1.1.1.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Originator: 3.3.3.3, Cluster list: 1.1.1.1
```

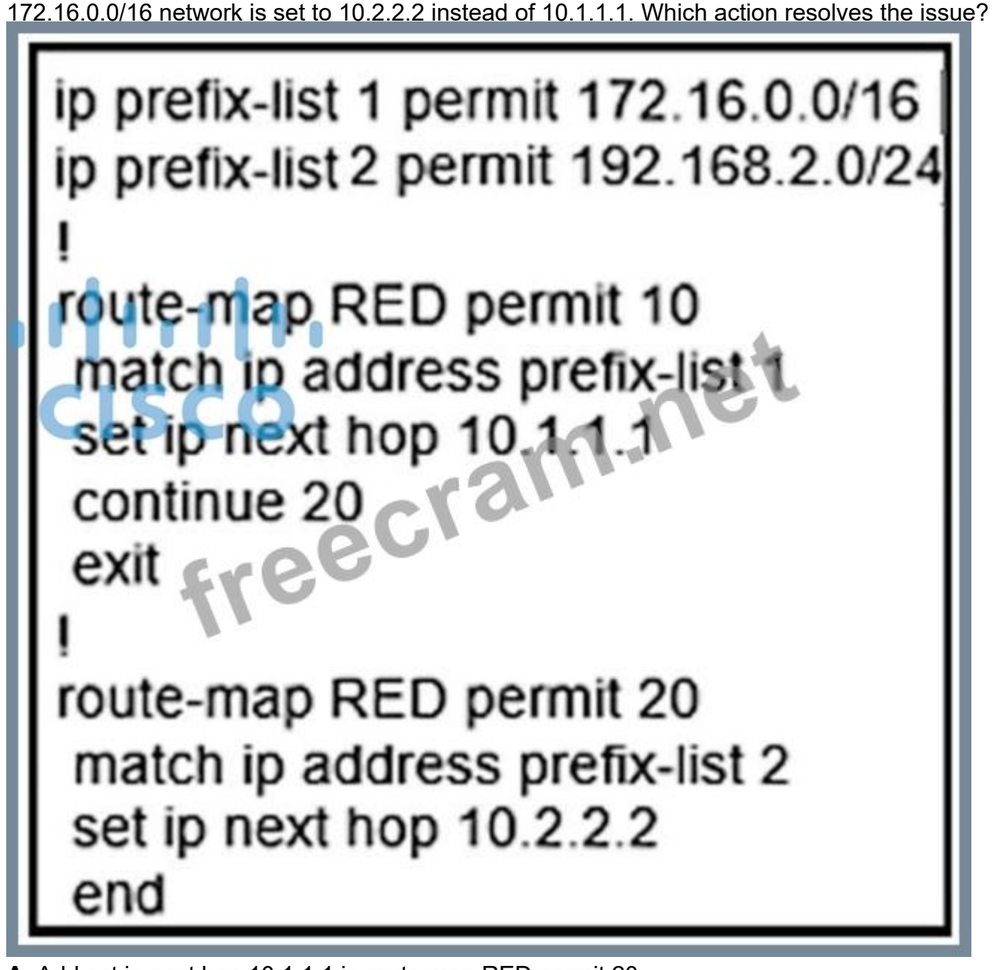
**A.** R1 is a route reflector client of a RR with a router ID of 1.1.1.1, and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to different ASs. The prefix is not advertised to any peer and must be advertised using the network statement on R3.
**B.** R1 is a route reflector 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
**C.** R1 is a route reflector with a router ID of 1.1.1.1, 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 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.
**Answer: (SHOW ANSWER)**
R1 is a route reflector client, and the prefix 2001:db8::1/128 is originated by a peer with the router ID of 3.3.3.3. Both R1 and the router with ID 3.3.3.3 are in the same AS, meaning they can share routes internally via the BGP Route Reflector (RR). The summarization must occur at the origin of the prefix (3.3.3.3) since that router is responsible for originating the more specific prefix (2001:db8::1/128).
To resolve, configure an aggregate address on the router with router ID 3.3.3.3 to summarize the specific prefix (2001:db8::1/128) into a broader /64 prefix:
router bgp <AS>
address-family ipv6
aggregate-address 2001:db8::/64 summary-only
This ensures that the summarized /64 prefix is advertised within the AS and to external peers while suppressing more specific routes.

**NEW QUESTION: 202**
Which protocol is used in a DMVPN network to map physical IP addresses to logical IP addresses?
**A.** LLDP
**B.** EIGRP
**C.** BGP
**D.** NHRP
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 203**
Which of the following are valid IPv6 Router Advertisement (RA) Guard modes? (Choose two.)
**A.** Open mode

**B.** Closed mode
**C.** Router mode
**D.** Guard mode
**E.** Host mode
**Answer: (SHOW ANSWER)**

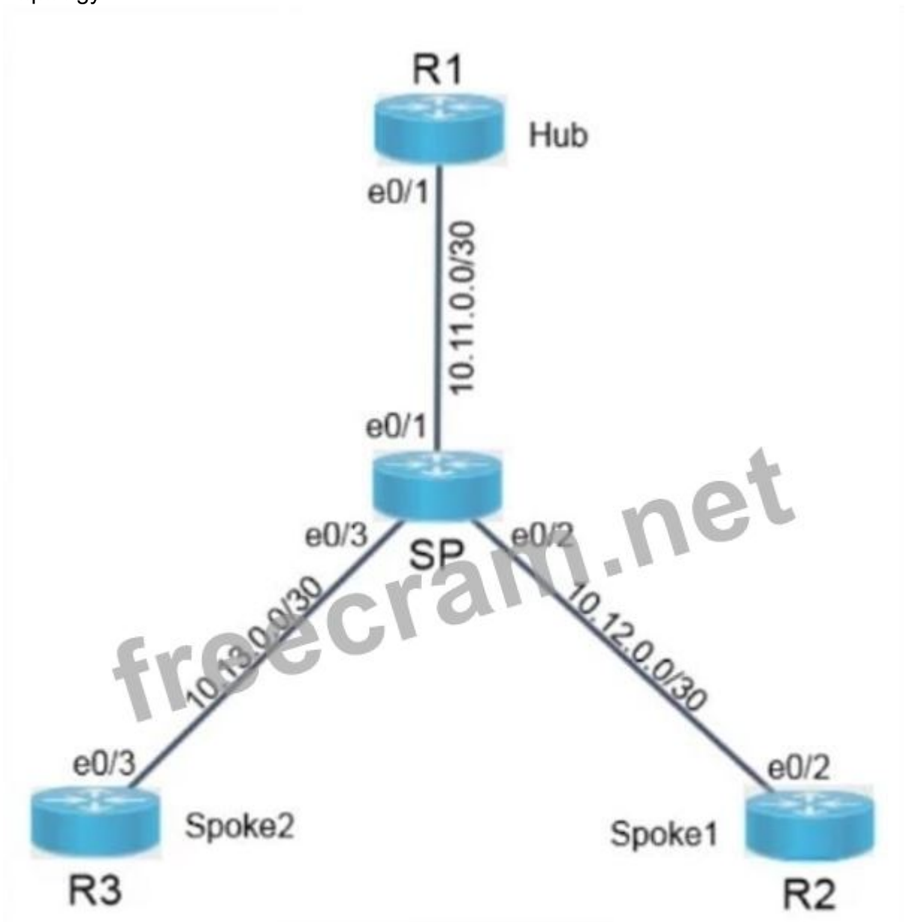
**NEW QUESTION: 204**
Refer to the exhibit. The forwarding entries how that the next hop for prefixes from the 172.16.0.0/16 network is set to 10.2.2.2 instead of 10.1.1.1. Which action resolves the issue?




**A.** Add set ip next hop 10.1.1.1 in route-map RED permit 20.
**B.** Add the continue statement in route-map RED permit 10 instead of continue 20.
**C.** Remove match ip address prefix-list 1 from route-map RED permit 10.
**D.** Remove the continue 20 statement from route-map RED permit 10
**Answer: (SHOW ANSWER)**
The continue statement causes processing to move to the next sequence, allowing the second clause to override the next-hop set in the first clause. Removing the continue ensures that once the first match occurs,

processing stops and the intended next hop is applied.

**NEW QUESTION: 205**
SIMULATION 19
Guidelines
Please use the "Tasks" and "Topology" tabs to complete this lablet.
Topology




| Device | Loopback 0 |
|---|---|
| R1 | 10.1.1.1/32 |
| R2 | 10.2.2.2/32 |
| R3 | 10.3.3.3/32 |



Tasks

R2 and R3 are pre-configured. Complete the configuration on R1 for these tasks:
Task 1
Complete the DMVPN phase 1 configuration on R1 to establish tunnel between R1-R2 and R1- R3. R1 must be configured to accept tunnel from any new spoke without additional configuration.
Do not remove existing configurations from any device.
Task 2
Configure R1 so that R2 and R3 learn each other networks advertised by EIGRP through the hub R1.
**Answer:**
Configure R1 as the DMVPN Phase 1 hub using multipoint GRE and NHRP, then run EIGRP on the tunnel so the hub advertises routes between the spokes.
R1

```
cisco
interface Tunnel0
 ip address <tunnel-ip> <mask>
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp map multicast dynamic
 no ip split-horizon eigrp <ASN>
 no ip next-hop-self eigrp <ASN>
```

```
cisco
router eigrp <ASN>
 no auto-summary
 network 10.1.1.1 0.0.0.0
 network <tunnel-network> <wildcard>
```

For DMVPN Phase 1, the hub must use tunnel mode gre multipoint so multiple spokes can connect to a single tunnel interface. ip nhrp map multicast dynamic allows the hub to accept multicast registrations dynamically from any new spoke, which means additional spoke tunnels can be learned without adding static NHRP mappings on the hub.
To let R2 and R3 learn each other's EIGRP routes through R1, EIGRP must run across the tunnel interface on the hub. Disabling EIGRP split horizon on the hub is required so routes learned from one spoke are advertised back out the same multipoint tunnel toward the other spoke. Disabling next-hop-self preserves proper spoke reachability behavior through the hub in the DMVPN environment.

**NEW QUESTION: 206**
A customer reports to the support desk that they cannot pnnt from their PC to the local printer id:401987778. Which tool must be used to diagnose the issue using Cisco DNA Center Assurance?
**A.** path trace
**B.** ACL trace
**C.** device trace
**D.** application trace
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 207**
Which protocol must be secured with MD-5 authentication across the MPLS cloud to prevent hackers from introducing bogus routers?
**A.** RSVP
**B.** ALSO
**C.** LDP
**D.** MP-BGP

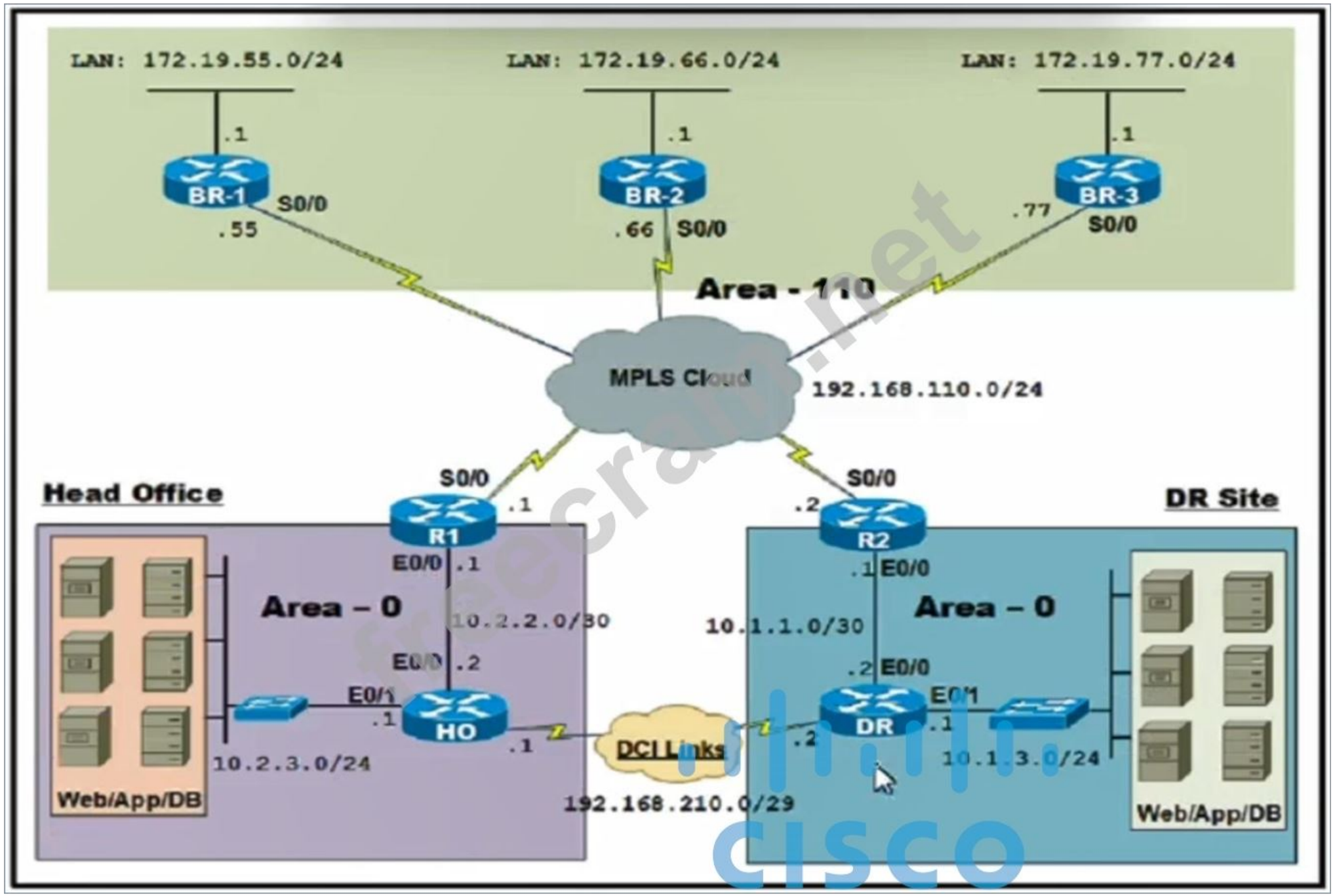
**Answer: (SHOW ANSWER)**

The Label Distribution Protocol (LDP) can also be secured with MD-5 authentication across the MPLS cloud. This prevents hackers from introducing bogus routers, which would participate in the LDP.

https://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/mpls/provisioning/guide/PGmpls1.html

**NEW QUESTION: 208**

Refer to the exhibit. During an unannounced link-maintenance window at the ISP, the DCI link went down, which caused a significant service outage. What action must the network engineer take at the head office to ensure Area-0 connectivity without intervention from the ISP?




**A.** Create a GRE tunnel interface in Area-0 between HO E0/0 and DR E0/0.
**B.** Create a virtual link in Area-0 between HO E0/0 and DR E0/0.
**C.** Create a GRE tunnel interface in Area-110 between R1 S0/0 and R2 S0/0.

**D.** Create a virtual link in Area-110 between R1 S0/0 and R2 S0/0.

**Answer: (SHOW ANSWER)**

In OSPF, all routers within an area must have full connectivity to avoid segmenting the area.

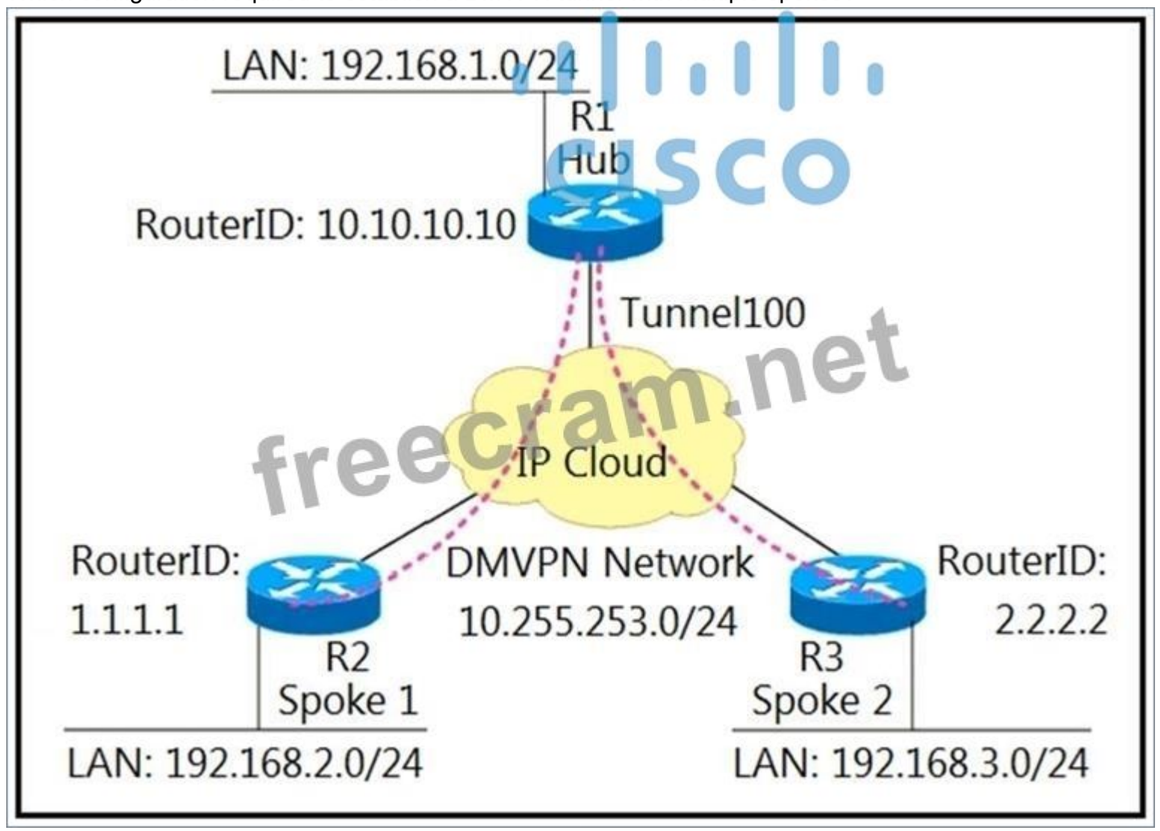
When the DCI (Data Center Interconnect) link went down, the connectivity between the two segments of Area-0 was lost, resulting in the service outage.

Creating a GRE (Generic Routing Encapsulation) tunnel between HO E0/0 and DR E0/0 allows logical connectivity for Area-0 traffic to flow through the MPLS cloud. The GRE tunnel encapsulates OSPF traffic, enabling Area-0 to maintain continuity without relying solely on the ISP's link.

**NEW QUESTION: 209**

Refer to the exhibit. A network administrator sets up an OSPF routing protocol for a DMVPN network on the hub router.

Which configuration required to establish a DMVPN tunnel with multiple spokes?

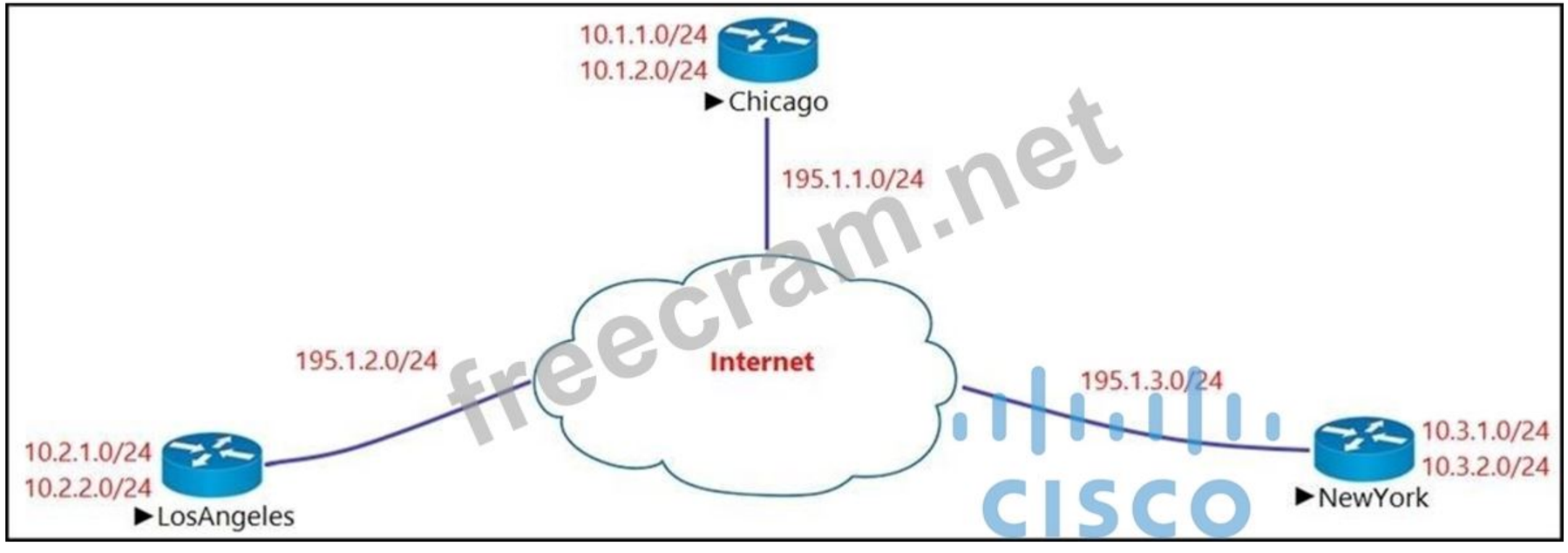


*Mar 1 17:19:04.051: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from LOADING to FULL, Loading Done
*Mar 1 17:19:06.375: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from FULL to DOWN, Neighbor Down: Adjacency forced to reset
*Mar 1 17:19:06.627: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from LOADING to FULL, Loading Done
*Mar 1 17:19:10.123: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from FULL to DOWN, Neighbor Down: Adjacency forced to reset
*Mar 1 17:19:14.499: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from LOADING to FULL, Loading Done
*Mar 1 17:19:19.139: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from EXSTART to DOWN, Neighbor Down: Interface down or detached
*Mar 1 17:01:51.975: %OSPF-4-NONEIGHBOR: Received database description from unknown neighbor 192.168.1.1
*Mar 1 17:01:57.783: OSPF: Rcv LS UPD from 192.168.1.1 on Tunnel100 length 88 LSA count 1
*Mar 1 17.01.57.155: OSPF: Send UPD to 10.255.253.1 on Tunnel100 length 100 LSA count 2

**A.** ip ospf network point-to-multipoint on both spoke routers
**B.** ip ospf network point-to-point on both spoke routers
**C.** ip ospf network point-to-point on the hub router
**D.** ip ospf network point-to-multipoint on One spoke router
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 210**
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?

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



Chicago

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source E0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp map multicast dynamic
 no ip next-hop-self eigrp 111
 tunnel protection ipsec profile IPSec-PROFILE
!
router eigrp 111
 network 192.168.1.0
 network 10.0.0.0
```

**A.** Interface Tunnel1
no ip split-horizon eigrp 111
**B.** Interface Tunnel1
Ip next-hop-self elgrp 111
**C.** Interface Tunnel1
tunnel mode Ipsec Ipv4
**D.** Interface Tunnel1
tunnel 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.

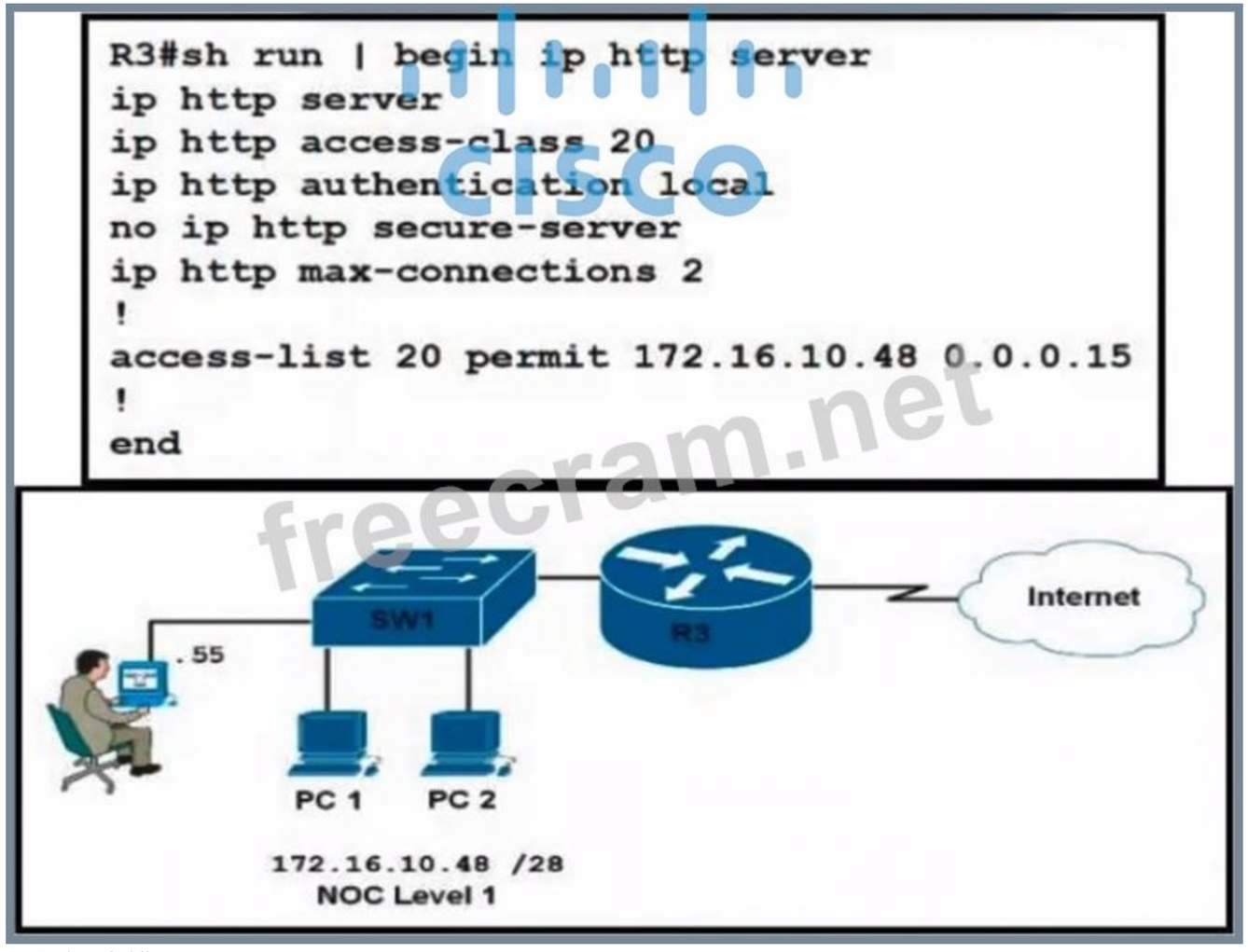
**NEW QUESTION: 211**
Refer to the exhibit. NTP is configured across the network infrastructure and Cisco DNA Center.
An NTP issue was reported on the Cisco DNA Center at 17:15. Which action resolves the issue?


**A.** Check and resolve reachability between the WLC and the NTP server
**B.** Reset the NTP server to resolve any synchronization issues tor 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.ht ml



**NEW QUESTION: 212**

Refer to the exhibit. Which configuration allows the operation level 1 team of 10 engineers to log in at least three at a time to router R3 using network credentials over HTTP?





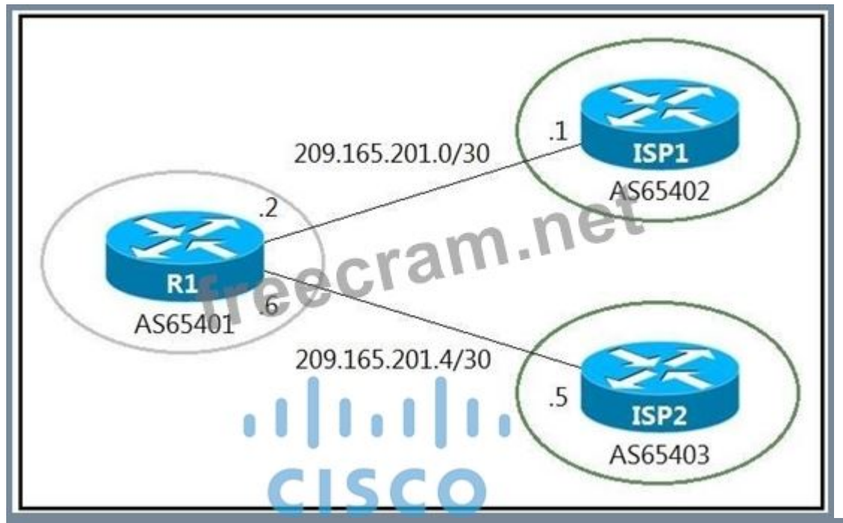

**A.** R3(config)#ip http authentication aaa
R3(config)#ip http max-connections 3
**B.** R3(config)#ip http max-connections 3
R3(config)#ip http accounting commands 3 default
**C.** R3(config)#ip http authentication enable
R3(config)#no access-list 20 permit 172.16.10.48 0.0.0.15
R3(config)#access-list 20 permit 172.16.10.48 0.0.0.7
**D.** R3(config)#ip http authentication aaa
R3(config)#no access-list 20 permit 172.16.10.48 0.0.0.15
R3(config)#access-list 20 permit 172.16.10.48 0.0.0.7
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 213**
Two MPLS routers, R1 and R2, are not directly connected and have an established LDP session running between them. What type of LDP session is this?
**A.** Remote LDP session
**B.** Tunneled LDP session
**C.** Targeted LDP session
**D.** Direct LDP session
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 214**
How does BFD protocol work?
**A.** BFD control packets are sent via UDP port 3784 to the destination router.
**B.** When BFD declares a failure on the primary IGP path, the router on the peer router chooses to use the secondary path.
**C.** BFD echo packets are sent to the same source IP and different destination IP with TCP port of
3786.
**D.** BFD operates on the route processor module and impacts the route processor CPU utilization.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 215**
Which IPv6 security feature blocks all traffic from an IPv6 host when initially connecting to a switch port except for traffic to gain an IPv6 address and discover IPv6 neighbors?
**A.** IPv6 Source Guard
**B.** IPv6 RA Guard
**C.** IPv6 DHCP Guard
**D.** IPv6 Destination Guard
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 216**
Refer to the exhibits. A company with autonomous system number AS65401 has obtained IP address block 209.165.200.224/27 from ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer in ISP1 reports that they are receiving ISP2 routes from AS65401.
Which configuration on R1 resolves the issue?




A.

```
R1#
 interface GigabitEthernet0/0
  ip address 209.165.201.2 255.255.255.252
 !
 interface GigabitEthernet0/1
  ip address 209.165.201.6 255.255.255.252
 !
 router bgp 65401
  bgp log-neighbor-changes
  redistribute static
  neighbor 209.165.201.1 remote-as 65402
  neighbor 209.165.201.5 remote-as 65403
 !
 ip route 209.165.200.224 255.255.255.224 Null0
 ip route 209.165.202.128 255.255.255.224 Null0
 !
```

```
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
 neighbor 209.165.201.1 distribute-list 10 out
```

**B.**

```
access-list 10 deny 209.165.202.128 0.0.0.31
 access-list 10 permit any
 !
router bgp 65401
  neighbor 209.165.201.1 distribute-list 10 in
```

**C.**

```
ip route 209.165.200.224 255.255.255.224 209.165.201.1
ip route 209.165.202.128 255.255.255.224 209.165.201.5
```

**D.**

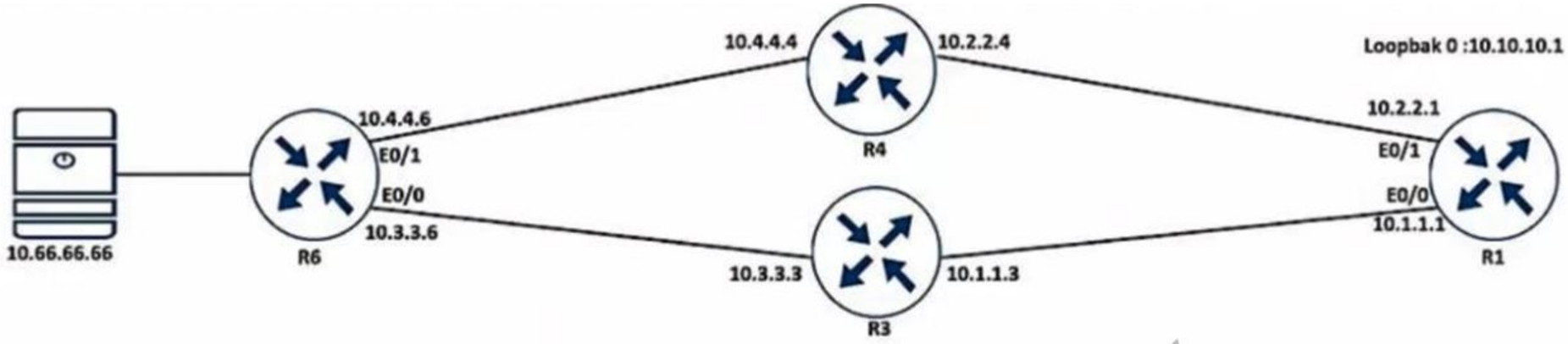
```
ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 0.0.0.0 0.0.0.0 100 209.165.201.5
```

**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 217**

Refer to the exhibit. A network administrator is trying to switch to the privileged EXEC level on R1 but failed. Which configuration resolves the issue?




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

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

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

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

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

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

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



**A.** tacacs-server enable-password Cisco@123
**B.** Enable password Cisco@123
**C.** enable-password Cisco@123
**D.** tacass server enable-password Cisco@123
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 218**
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: 219**
How long is the default NHRP cache timer?
**A.** 30 minutes
**B.** 2 hours
**C.** 1 hour
**D.** 15 minutes
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 220**
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: 389362063 packets, 222009685077 bytes
```

What are the two effects of th s 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)**

In the sequence 5 of route-map PBR, all the packets matched access-list NON-CISCO will be dropped (by "deny" statement). But from the "Policy routing matches: 0 packets, 0 bytes" line, we can deduce no packets have been dropped so far.
In the sequence 10 of route-map PBR, if a match command is not present then all routes match the clause. Therefore all other packets will be matched by sequence 10 and they are forwarded to the default gateway 192.168.1.5.
https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html

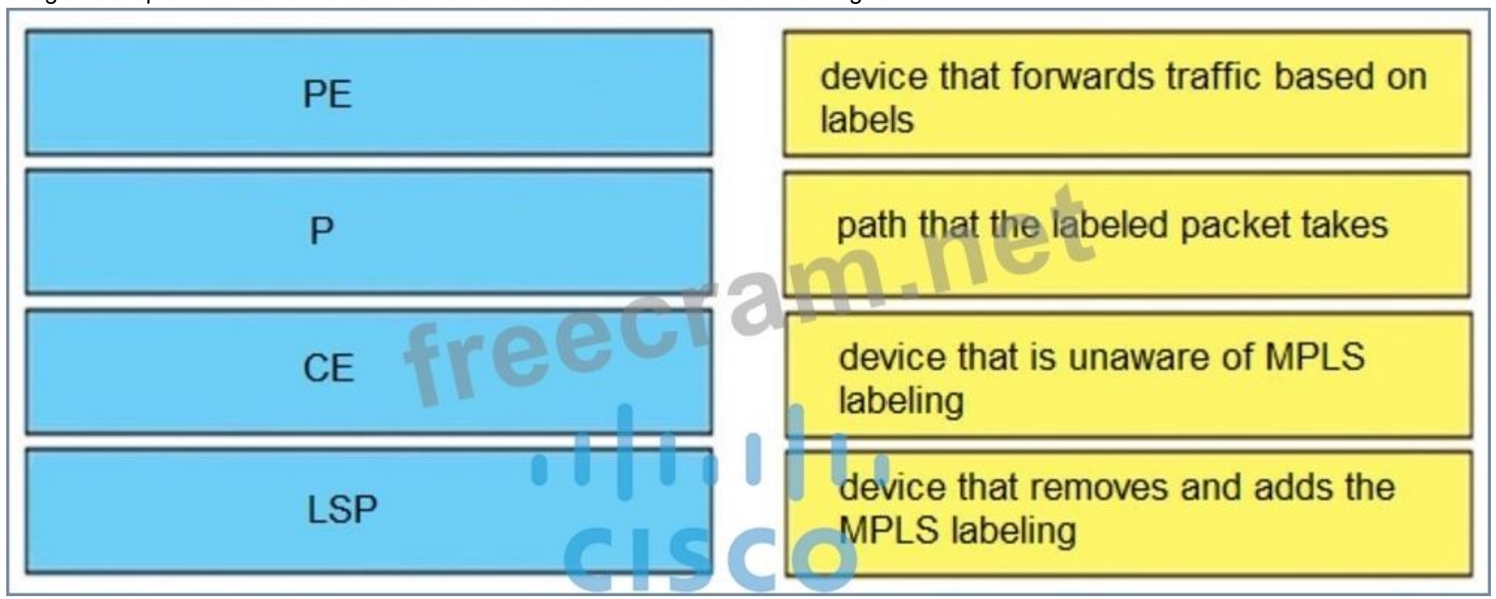
**NEW QUESTION: 221**
Refer to the exhibit. An engineer is investigating an OSPF issue reported by the Cisco DNA Assurance Center. Which action resolves the issue?


**A.** One of the interfaces is using the wrong MTU Match interface MTU on both links
**B.** An ACL entry blocking multicast on the interfaces Allow multicast through the interface ACL
**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: (SHOW ANSWER)**

**NEW QUESTION: 222**
Which of the following correctly describes the concept of split horizon with IP routing? (Choose two.)
**A.** Split horizon is used to filter customer routes in an ISP network.
**B.** Split horizons cannot be disabled on WAN interfaces
**C.** Split horizon is a valid routing loop prevention mechanism
**D.** Split horizon is not applicable to EIGRP networks
**E.** When enabled, split horizons informs the router to not advertise routes back out the same interface from where that route was originally received.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 223**
An engineer failed to run diagnostic commands on devices using Cisco Catalyst Center (formerly DNA Center). Which action in Cisco Catalyst Center resolves the issue?
**A.** Enable Command Runner
**B.** Enable APIs
**C.** Enable CDP
**D.** Enable Secure Shell
**Answer: A (LEAVE A REPLY)**
The Command Runner feature in Cisco Catalyst Center must be enabled to allow the platform to execute CLI diagnostic commands on managed devices. Enabling Command Runner restores the ability to push and retrieve command output.

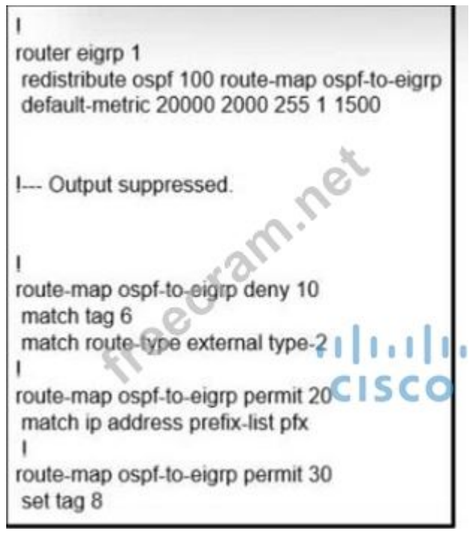
**NEW QUESTION: 224**
Drag and Drop Question
Drag and drop the MPLS terms from the left onto the correct definitions on the right.





**NEW QUESTION: 225**
What is an advantage of using BFD?
**A.** It detects local link failure at layer 1 and updates routing table.
**B.** It detects local link failure at layer 2 and updates routing protocols.
**C.** It has sub-second failure detection for layer 1 and layer 3 problems.
**D.** It has sub-second failure detection for layer 1 and layer 2 problems.
**Answer: (SHOW ANSWER)**
BFD provides rapid, sub-second failure detection independent of the underlying protocol and works across Layer 3, allowing routing protocols to quickly react to both Layer 1 and Layer 3 failures.

**NEW QUESTION: 226**
Refer to the exhibit. Which action fixes the OSPF routes redistribution into EIGRP?




**A.** Match external type to type-1

**B.** Set tags before matching into EIGRP

**C.** Set a default metric in the route map

**D.** Match OSPF and EIGR IDs

**Answer: (SHOW ANSWER)**

The current configuration in the exhibit shows redistribution of OSPF into EIGRP with a route map called ospf-to-eigrp. The route map has the following sequence:

Sequence 10: Denies routes with a tag of 6 and an OSPF route type of "external type-2." Sequence 20: Permits routes that match a prefix list pfx.

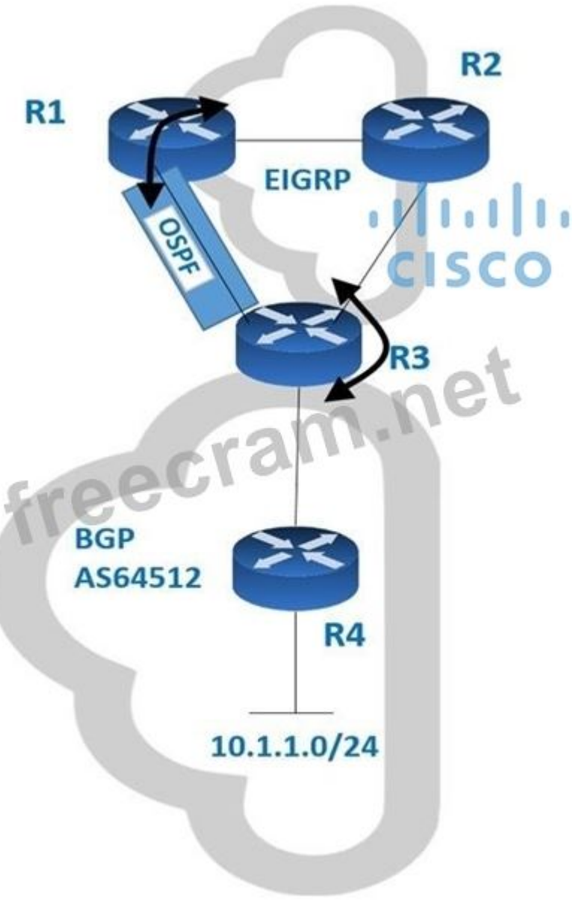
Sequence 30: Permits all other routes and sets the tag to 8.

Matching "external type-1" instead of "external type-2" in the route map could fix the issue by allowing specific types of external OSPF routes to be redistributed into EIGRP, which may be necessary depending on the route requirements.



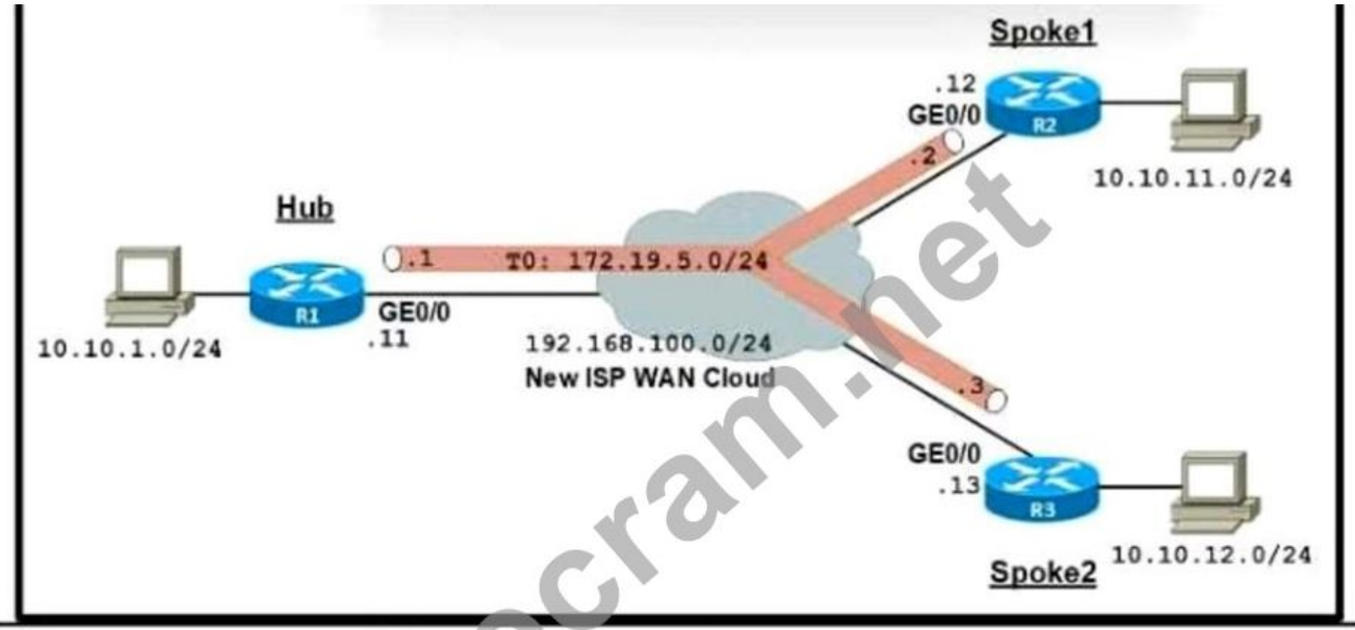
**NEW QUESTION: 227**

Refer to the exhibit. BGP and EIGRP are mutually redistributed on R3, and EIGRP and OSPF are mutually redistributed on R1. Users report packet loss and interruption of service to applications hosted on the 10.1.1.0724 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)**
As it states in the debug "Connection refused by remote host".
Extra step needed on the remote router (R3) which is to activate the neighbor in address-family ipv6 unicast and run the "neighbor <neighbor_IP> activate" command.

**NEW QUESTION: 228**
Refer to the exhibit. An organization is installing a new L3 MPLS link to establish DMVPN Phase
2 tunnels between the hub and two spoke routers. Which additional configuration should the engineer implement on each device to achieve optimal routing between the spokes?




R1
```
interface Tunnel0
   ip address 172.19.5.1 255.255.255.0
   ip nhrp authentication t@li$C0
   ip nhrp map multicast dynamic
   ip nhrp network-id 10
   ip ospf network broadcast
   ip ospf priority 255
   tunnel source 192.168.100.11
   tunnel mode gre multipoint
   tunnel key 100
```

R2
```
interface Tunnel0
   ip address 172.19.5.2 255.255.255.0
   ip nhrp authentication t@li$C0
   ip nhrp map multicast 192.168.100.11
   ip nhrp map 172.19.5.1 192.168.100.11
   ip nhrp network-id 10
   ip ospf network broadcast
   ip ospf priority 0
   tunnel source 192.168.100.12
   tunnel destination 192.168.100.11
   tunnel key 100
```

R3
```
interface Tunnel0
   ip address 172.19.5.3 255.255.255.0
   ip nhrp authentication t@li$C0
   ip nhrp map multicast 192.168.100.11
   ip nhrp map 172.19.5.1 192.168.100.11
   ip nhrp network-id 10
   ip ospf network broadcast
   ip ospf priority 0
   tunnel source 192.168.100.13
   tunnel destination 192.168.100.11
   tunnel key 100
```

A.
```
interface Tunnel0
  ip ospf priority 1
  ip ospf network non-broadcast
```

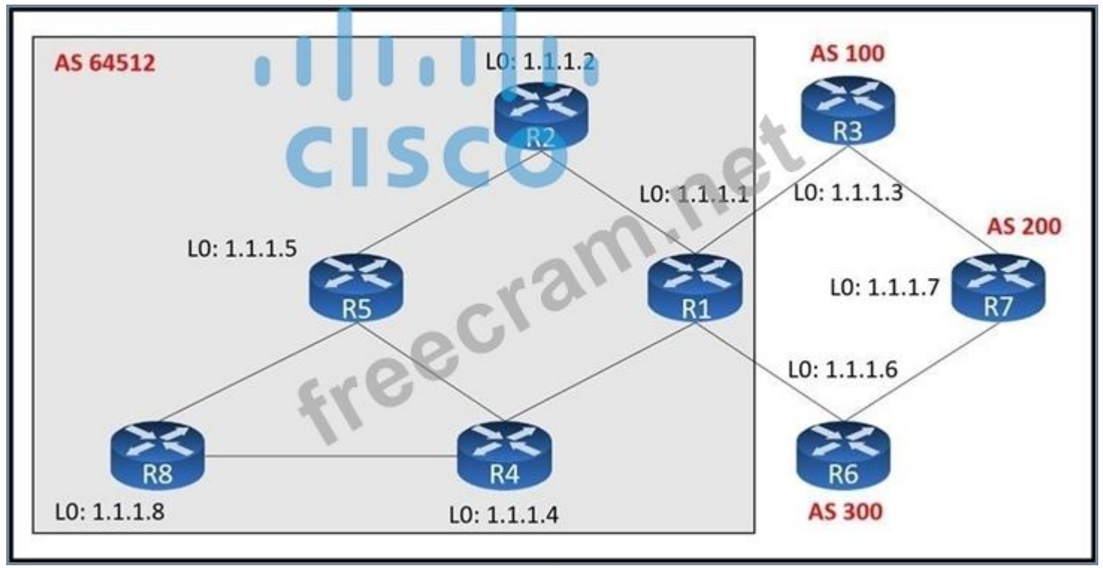
B.
```
interface Tunnel0
  no tunnel destination 192.168.100.11
  tunnel mode gre multipoint
```

C.
```
interface Tunnel0
  no tunnel destination 192.168.100.11
  tunnel mode mpls traffic-eng
```

D.
```
interface Tunnel0
  ip ospf priority 253
  ip ospf network point-to-multipoint
```

**Answer: B (LEAVE A REPLY)**
There is no need for tunnel destination and we need gre multipoint tunnel mode The OSPF priority of hub must be higher than the priority of spokes.
https://networklessons.com/cisco/ccie-routing-switching/dmvpn-phase-2-basic-configuration
https://networklessons.com/cisco/ccie-routing-switching/dmvpn-phase-2-ospf-routing

**NEW QUESTION: 229**
Refer to the exhibit. An engineer configured R2 and R5 as route reflectors and noticed that not all routes are sent to R1 to advertise to the eBGP peers. Which iBGP routers must be configured as route reflectors to advertise all routes to restore reachability across all networks?




**A.** R1 and R4
**B.** R1 and R5
**C.** R4 and R5
**D.** R2 and R5
**Answer: (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. Thereforesome routes are missing on R1 to advertise to eBGP peers.
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: 230**
Which statement about MPLS LDP router ID is true?
**A.** The force keyword changes the router ID to the specific address causing any impact.
**B.** The loopback with the highest IP address is selected as the router ID.
**C.** If not configured, the operational physical interface is chosen as the router ID even if a loopback is configured.
**D.** If MPLS LDP router ID must match the IGP router ID.
**Answer: B (LEAVE A REPLY)**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4m/mp-ldp-12-4m- book.pdf

**NEW QUESTION: 231**
How are CE advertised routes segmented from other CE routers on an MPLS PE router?
**A.** by assigning CE-facing interfaces to different VRFs
**B.** with a combination of VRF-Lite and MP-BGP
**C.** by pushing MPLS labels advertised by LDP on customer routes
**D.** by enabling multiple instances of BGP, one for each CE router
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 232**
Refer to the exhibit. The authentication is not working as desired and the user drops into user- exec mode.
Which configuration resolves the issue?

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

**A.** aaa new-model
aaa authentication common-id default local
aaa authorization exec default local
!
line vty 0 4
login authentication default
authorization exec default
**B.** aaa new-model
aaa authentication login local
aaa authorization exec local
!
line vty 0 4
login authentication local
authorization exec default

**C.** aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
line vty 0 4
login authentication default
authorization exec default
**D.** aaa new-model
aaa authentication login default local
aaa authorization priv default 15
!
line vty 0 4
login authentication default
authorization exec priv15
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 233**
Refer to the exhibit. Which configuration resolves the issue?

```
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0          1         no          no          Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.100.7, Interface address 172.16.1.42
  Backup Designated router (ID) 172.16.100.5, Interface address 172.16.1.41
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01

 Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 172.16.100.5  (Backup Designated Router)
 Suppress hello for 0 neighbor(s)
 Cryptographic authentication enabled
   Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain ospf
   Rollover in progress, 1 neighbor(s) using the old key(s):
     key id 1 algorithm MD5
CSR103#
CSR103#
CSR103#sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.100.3      1   FULL/DR         00:00:30    172.16.1.25     GigabitEthernet3
172.16.100.5      1   FULL/BDR        00:00:16    172.16.1.41     GigabitEthernet2
CSR103#
CSR103#
CSR103#
*Jan 11 16:49:35.311: %SYS-6-LOGOUT: User admin has exited tty session 1(10.228.200.250)
*Jan 11 16:49:45.396: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.100.5 on GigabitEthernet2 from
 FULL to DOWN, Neighbor Down: Dead timer expired
```

A.
```
int GigabitEthernet 2
  ip ospf message-digest-key 1 md5 cisco
  ip ospf authentication message-digest
```

B.
```
key chain ospf
  key 1
    key-string 7 02050D480809
       cryptographic-algorithm hmac-sha-1
interface GigabitEthernet2
  ip ospf authentication key-chain ospf
```

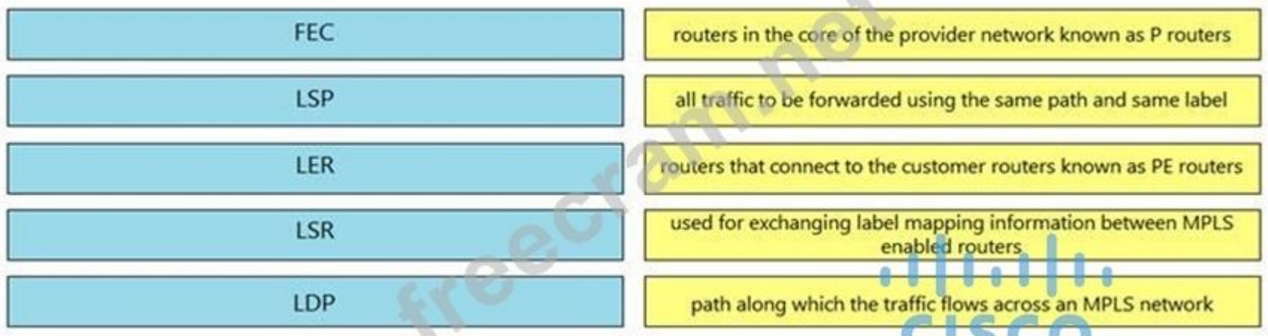
C.
```
router ospf 1
  area 1 authentication message-digest
 int GigabitEthernet 2
  ip ospf message-digest-key 1 md5 cisco
```

D.
```
int GigabitEthernet 2
  ip ospf key 1 cisco
  ip ospf authentication
```

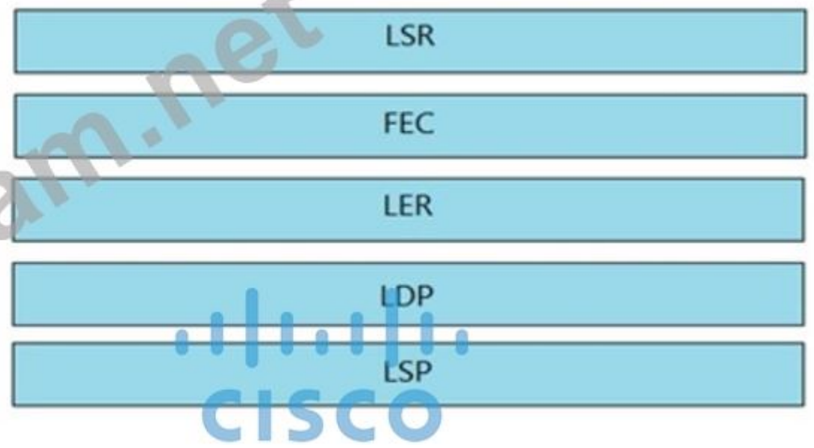
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 234**
Which description characterizes the primary purpose of route target (RT) in a Multiprotocol Label Switching (MPLS) network?
**A.** RT is a unique identifier assigned to each VPN route in an MPLS network.
**B.** RT is a parameter used to prioritize routing decisions in an MPLS network.
**C.** RT is a mechanism used to control the distribution of VPN routes between different VPN sites in an MPLS network.
**D.** RT is a label assigned to packets to facilitate efficient routing in an MPLS network.
**Answer: (SHOW ANSWER)**
Route targets are BGP extended communities used to control which VPN routes are imported and exported between VRFs. They define the membership of VPN routes, ensuring that only the intended sites receive specific routes across the MPLS network.

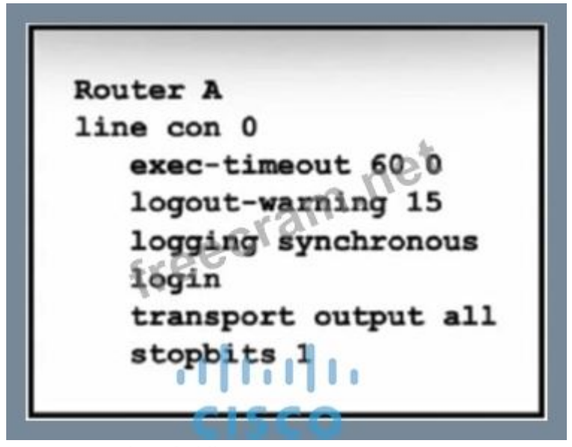
**NEW QUESTION: 235**
Drag and Drop Question
Drag and drop the descriptions from the left onto the corresponding MPLS components on the right.




**Answer:**

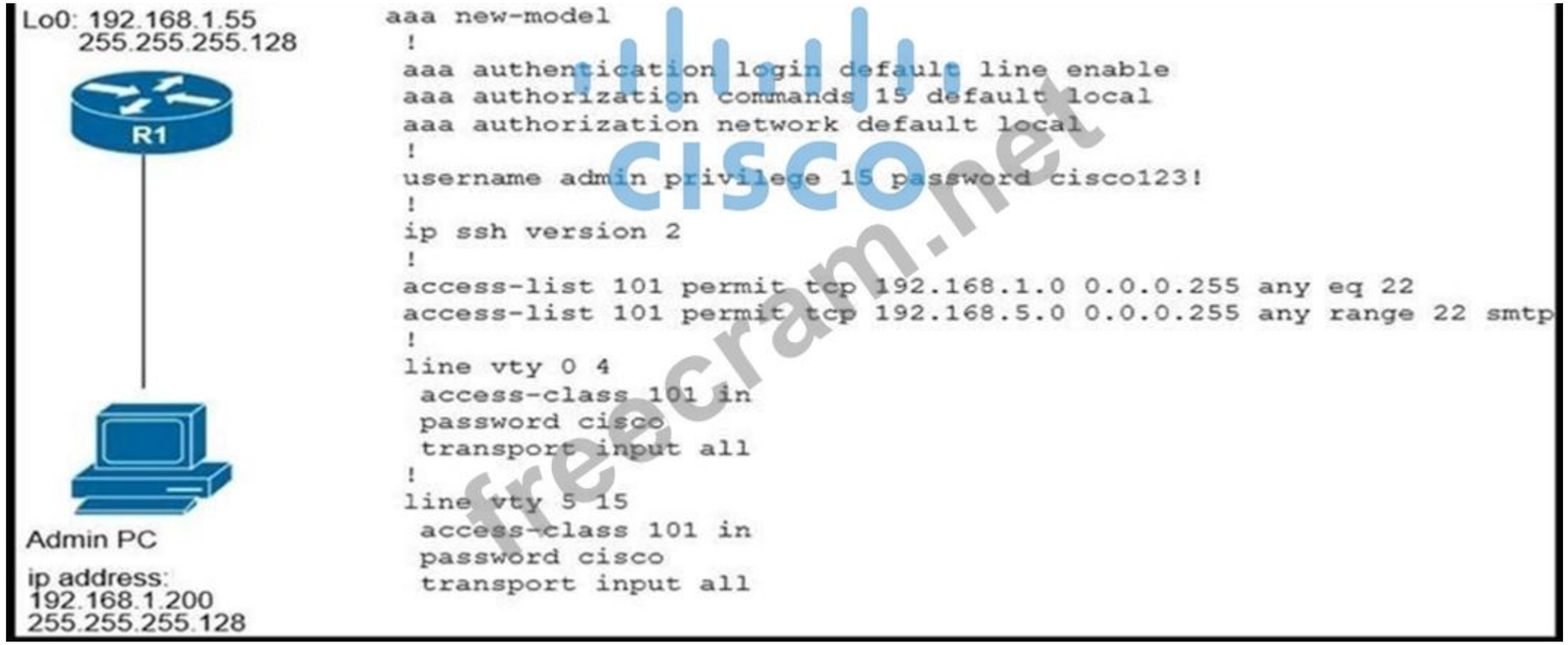



**NEW QUESTION: 236**
Refer to the exhibit. After a misconfiguration by a junior engineer, the console access to router A is not working. Which configuration allows access to router A?




**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-line)#login local
RouterA(config)#end
**C.** RouterA(config)#aaa new-model
RouterA(config)#line console 0
RouterA(config-line)#login authentication CONSOLE
**D.** RouterA(config)#line console 0
RouterA(config-line)#password cisco
RouterA(config)#end
**Answer: (SHOW ANSWER)**
The misconfiguration has likely caused the console access to fail due to a missing or incorrect password configuration. The configuration in Option D sets a simple password (cisco) on the console line and does not require additional AAA configurations or login methods.

**NEW QUESTION: 237**
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.** secret cisco123! at the end of the username command instead of password cisco123!

**B.** aaa authorization reverse-access

**C.** matching password on vty lines as cisco123!

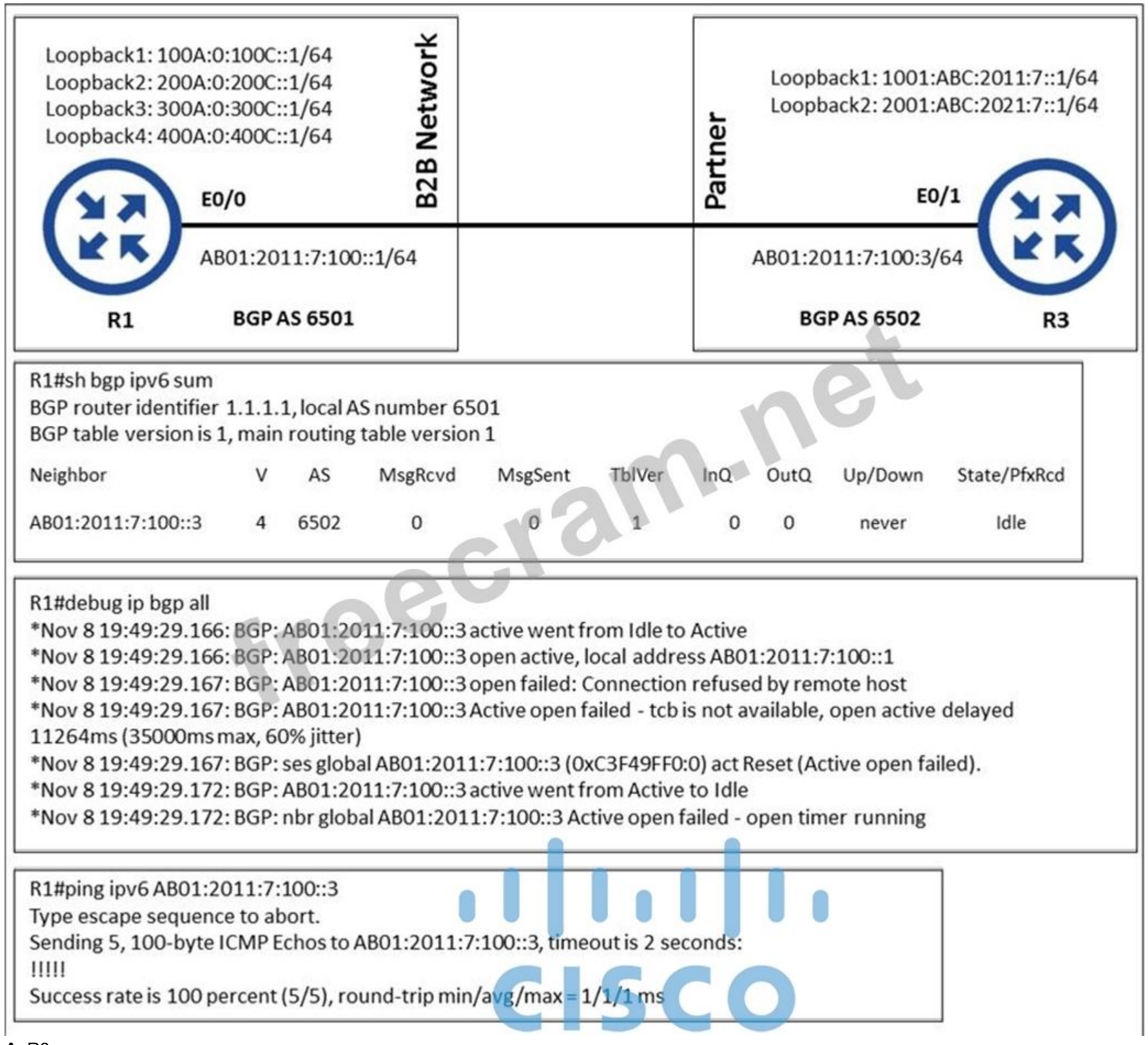
**D.** enable secret or enable password commands to enter into privileged mode

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 238**

An engineer configured BGP between routers R1 and R3. The BGP peers cannot establish neighbor adjacency to be able to exchange routes.

Which configuration resolves this issue?




**A.** R3

router bgp 6502

address-family ipv6
neighbor AB01:2011:7:100::1 activate
**B.** R1
router bgp 6501
address-family ipv6
neighbor AB01:2011:7:100::3 activate
**C.** R3
router bgp 6502
neighbor AB01:2011:7:100::1 ebgp-muttlhop 255
**D.** R1
router bgp 6501 neighborAB01:2011:7:100::3ebgp-multihop255
**Answer: (SHOW ANSWER)**
As it states in the debug "Connection refused by remote host".
Extra step needed on the remote router (R3) which is to activate the neighbor in address-family ipv6 unicast and run the "neighbor <neighbor_IP> activate" command.

**NEW QUESTION: 239**
Refer to the exhibit. The router is redistributing a prefix 172.16.10.0/24 that should have been filtered. Which action resolves the issue?

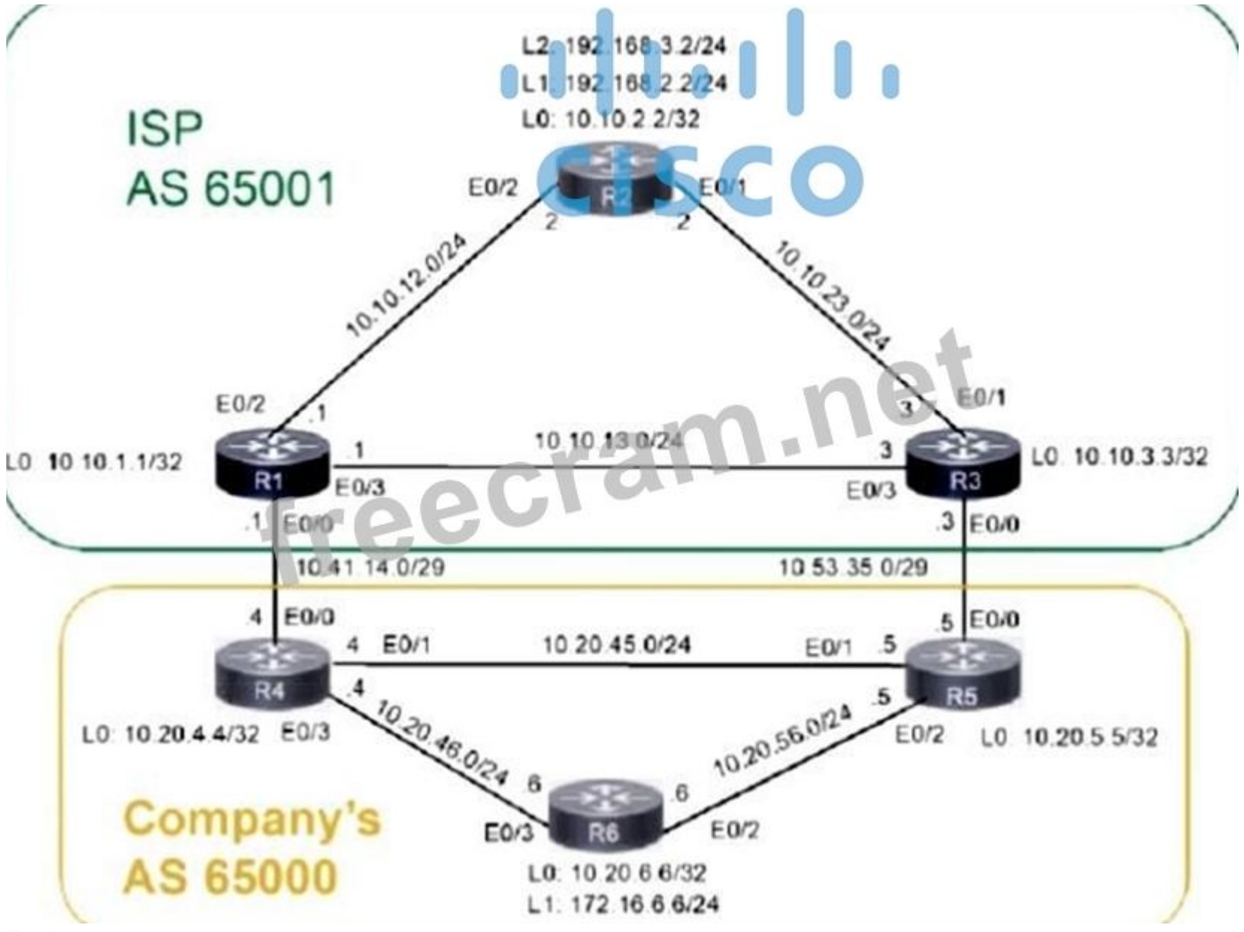
```
t1# show route-map
oute-map Redistribution_EIGRP, permit, sequence 1(
 Match clauses:
   ip address (access-lists): 10
 Set clauses:
   tag 666
 Policy routing matches: 0 packets, 0 bytes
oute-map Redistribution_EIGRP, permit, sequence 2(
 Match clauses:
 Set clauses:
 Policy routing matches: 0 packets, 0 bytes

t1# show access-lists
Standard IP access list 10
    10 permit 172.16.1.0, wildcard bits 0.0.0.255
    20 permit 172.16.2.0, wildcard bits 0.0.0.255
```

**A.** Match the tag 666 for the route in the route map.
**B.** Remove route-map sequence 20.
**C.** Add the route in access-list 10.
**D.** Permit the route in route-map sequence 20.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 240**
LAB SIMULATION 6
Guidelines
This is a lab item in which tasks will be performed on virtual devices.
* Refer to the Tasks tab to view the tasks for this lab item.

* Refer to the Topology tab to access the device console(s) and perform the tasks.
* Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
* All necessary preconfigurations have been applied.
* Do not change the enable password or hostname for any device.
* Do not replace existing routing policies or configurations.
* Save your configurations to NVRAM before moving to the next item.
* Click Next at the bottom of the screen to submit this lab and move to the next question.
* When Next is clicked, the lab closes and cannot be reopened.

Topology




Tasks

A company is connected to an ISP and some of the networks between the ISP and the company are not reachable. Troubleshoot and resolve the issues to achieve these goals:

1. A single /16 is advertised for all infrastructure-connected interfaces that belong to the 10.20.x.x network using BGP network commands from border routers connected to the ISP. Configuration modification is allowed in R4 and R5 to achieve the results. Do not use the BGP aggregate command.
2. R6 receives the ISP R2 Loopback2 from R4 and receives a summary address for both Loopbacks of ISP R2 from R4 or R5. Use BGP attribute local-preference, add , for example, for R6, use "default+6 = value to be used". Use the existing prefix lists or route maps with the sequence numbering starting at 10 and added in increments of 10.
3. R6 receives the ISP R2 Loopback1 from R5 and receives a summary address for both Loopbacks of ISP R2 from R4 or R5 using the same guidelines.

4. R6 advertises its Loopback1 /24 address through BGP.

**Answer:**

R4:

```
R4# config t
R4(config)# ip route 10.20.0.0 255.255.0.0 null 0
R4(config)# no ip prefix-list AS65001-in
R4(config)# ip prefix-list AS65001-in seq 10 permit 192.168.2.0/24
R4(config)# route-map AS65001-in permit 20
R4(config-route-map)# set local-preference 104
R4(config-route-map)# end
R4# clear ip bgp * soft
R4# wr
```

R5:

```
R5# config t
R5(config)# ip route 10.20.0.0 255.255.0.0 null 0
R5(config)# no ip prefix-list AS65001-in
R5(config)# ip prefix-list AS65001-in seq 10 permit 192.168.3.0/24
R5(config)# route-map AS65001-in permit 20
R5(config-route-map)# set local-preference 105
R5(config-route-map)# end
```

R5# clear ip bgp * soft R5# wr

R6:

R6# config t

R6(config-router)# address-family ipv4

R6(config)# router bgp 65000

R6(config-router-af)# no network 172.16.6.0

R6(config-router-af)# network 2.16.6.0 mask 255.255.255.0

R6(config-router-af)#

R6# wr mem

**NEW QUESTION: 241**
What is the role of LDP in MPLS networks?
**A.** It enables label binding that exchanges route descriptors.
**B.** It disables label binding information to exchange with peer LSRs.
**C.** It creates MPLS packet forwarding along with the IGP routes.
**D.** It enables label binding information to exchange with peer LSRs.
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 242**
A network administrator is reloading a router and during the bootup, he is getting the error message "%Error opening tftp://255.255.255.255/network-confg (Socket error)". What command need to be applied on Cisco Router to fix this issue.
**A.** No service config
**B.** Reload noconfirm
**C.** Write erase reload

**D.** Copy run start
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 243**


oting IPv6 address assignment for a DHCP client that is not getting an IPv6 address from the server.

Which configuration retrieves the client IPv6 address from the DHCP server?
**A.** ipv6 address autoconfig command on the interface
**B.** ipv6 dhcp server automatic command on DHCP server
**C.** ipv6 dhcp relay-agent command on the interface

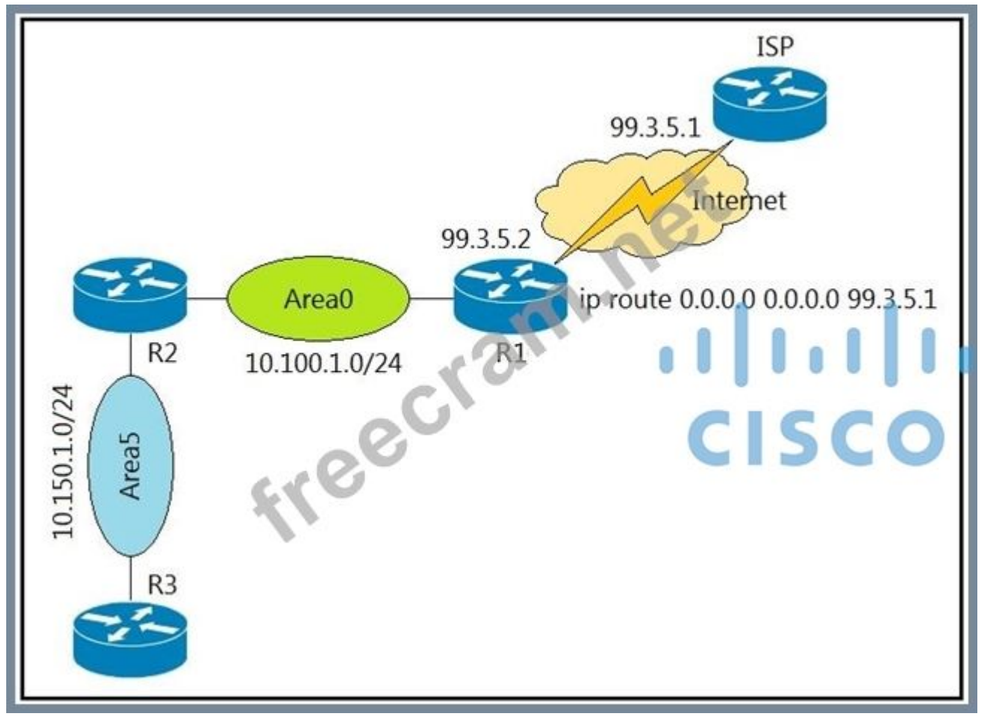
**D.** service dhcp command on DHCP server

**Answer: (SHOW ANSWER)**

The first step is using the ipv6 address autoconfig to create the link-local address for the interface, then the ip address will be assign to the interface using dhcp server, and the command is "ipv6 address dhcp".

**NEW QUESTION: 244**

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




**A.** router ospf 1
default-information originate

**B.** router ospf 1
network 0.0.0.0 0.0.0.0 area 0

**C.** router ospf 1
redistribute connected 0.0.0.0

**D.** router ospf 1
redistribute static subnets

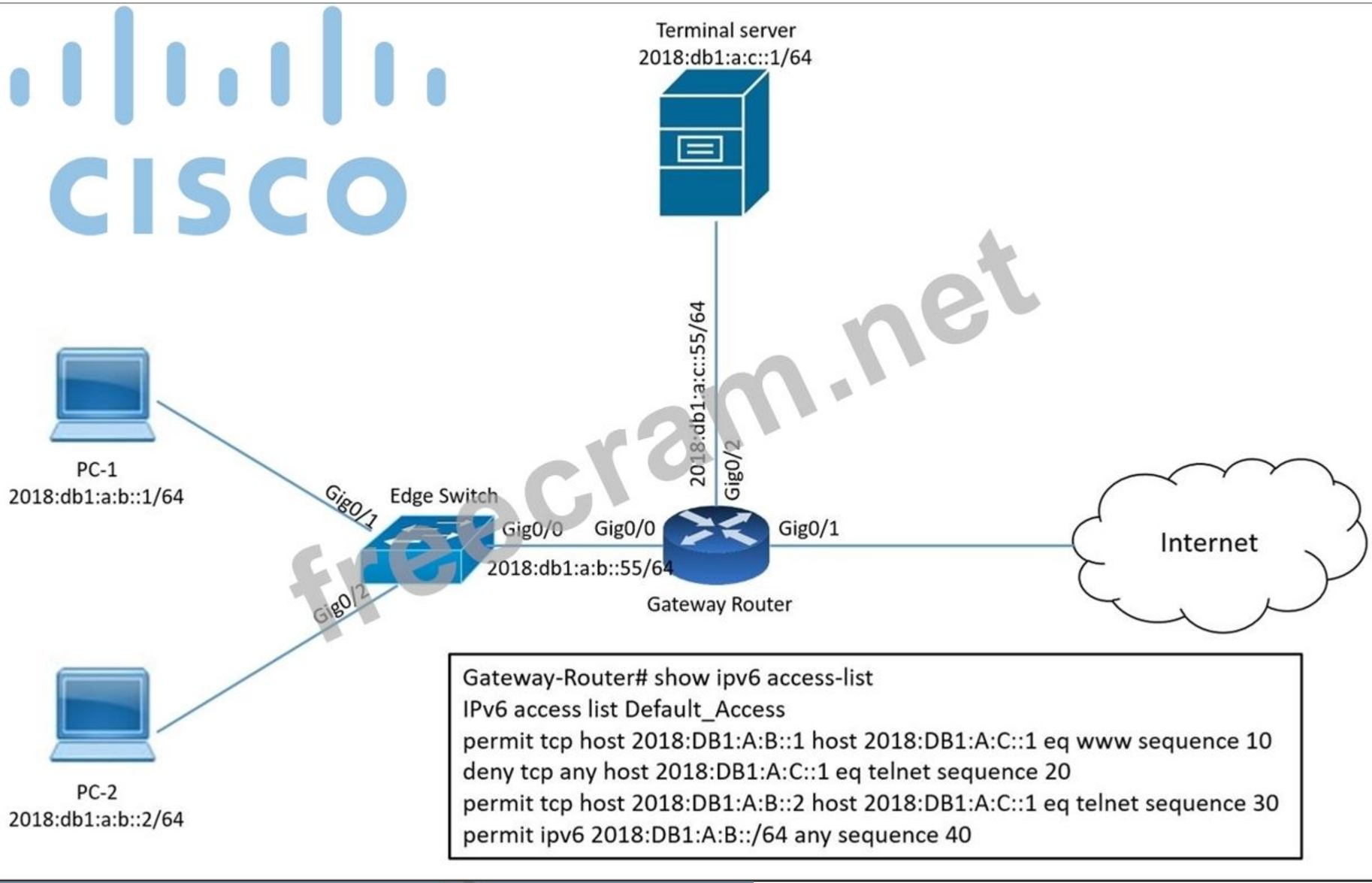
**Answer: (SHOW ANSWER)**

To advertise the existing default static route into OSPF, the correct command is default- information originate. This injects a default route into OSPF so internal routers can use R1 as the path to the Internet.

**NEW QUESTION: 245**

Refer to the exhibit. PC-2 failed to establish a Telnet connection to the terminal server.

Which configuration resolves the issue?




```
Gateway-Router(config)#ipv6 access-list Default_Access
Gateway-Router(config-ipv6-acl)#sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet

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

Gateway-Router(config)#ipv6 access-list Default_Access
Gateway-Router(config-ipv6-acl)#no sequence 20
Gateway-Router(config-ipv6-acl)#sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet

Gateway-Router(config)#ipv6 access-list Default_Access
Gateway-Router(config-ipv6-acl)#sequence 25 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
```

**A.** Option A
**B.** Option B
**C.** Option C
**D.** Option D
**Answer: (SHOW ANSWER)**
In fact in this question both answer A and answer C are correct but we believe answer A is the better choice as it only allows PC-2 to telnet to terminal server. All other hosts are refused to telnet to terminal server via sequence 20.

**NEW QUESTION: 246**
Refer to the exhibit. A client is concerned that passwords are visible when running this show archive log config all.

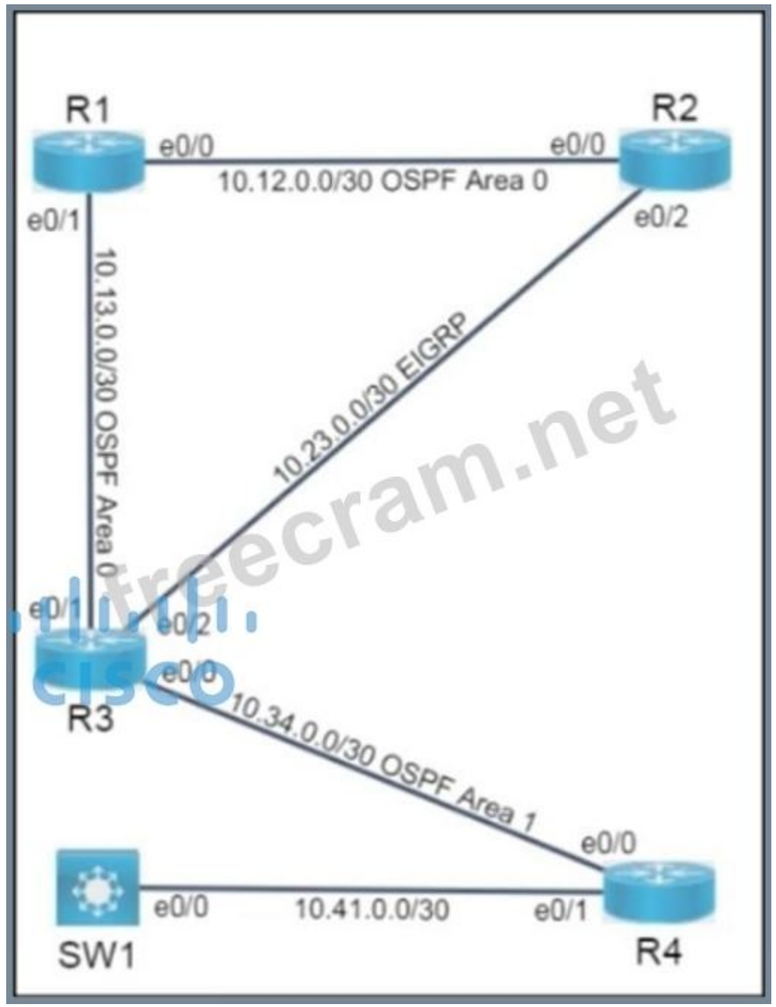
```
MASS-RTR#show running-config
!
hostname MASS-RTR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization commands 15 default local
!
username admin privilege 15 password 7 02362448181l5F3348
username cisco privilege 15 password 7 0607072C494A5B
archive
  log config
   logging enable
   logging size 1000
!
interface GigabitEthernet0/0
  ip address dhcp
  duplex auto
  speed auto
!
line vty 0 4
!

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

Which router configuration is needed to resolve this issue?
**A.** MASS-RTR(config-archive-log-cfg)#hidekeys

**B.** MASS-RTR(config-archive-log-cfg)#password encryption aes
**C.** MASS-RTR(config)#service password-encryption
**D.** MASS-RTR(config)#aaa authentication arap
**Answer: (SHOW ANSWER)**




**NEW QUESTION: 247**
SIMULATION 17
Guidelines
This is a lab item in which tasks will be performed on virtual devices.
Refer to the Tasks tab to view the tasks for this lab item.
Refer to the Topology tab to access the device console(s) and perform the tasks.
Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
All necessary preconfigurations have been applied.
Do not change the enable password or hostname for any device.
Save your configurations to NVRAM before moving to the next item.
Click Next at the bottom of the screen to submit this lab and move to the next question.
When Next is clicked, the lab closes and cannot be reopened.
Topology






Tasks

Complete the tasks below.

Task 1

Ensure that R3's loopback is received via EIGRP on R2. Do not modify the EIGRP default administrative distance to achieve this task.

Task 2

Ensure that Area 1 can accept redistributed routes while blocking Type 5 LSAs. Upon completion, R3's Loopback should be seen on R4 learned via OSPF.

Task 3

Configure R3 so that traffic sourced from R4's Loopback 0 IP address destined to R2's Loopback

0 IP address will always use the path between R3 and R1. Use an ACL and route map named

"PBR" to achieve this task.


**Answer:**

On R3, advertise Loopback0 directly into EIGRP so R2 learns it as an internal EIGRP route, configure OSPF Area 1 as NSSA and redistribute the loopback into OSPF, then use PBR inbound on the interface toward R4.

R3

```
cisco

router eigrp 100
 network <R3_Loopback0_IP> 0.0.0.0

router ospf 1
 area 1 nssa
 redistribute connected subnets route-map LOOPBACK_INTO_OSPF

route-map LOOPBACK_INTO_OSPF permit 10
 match interface Loopback0

access-list 101 permit ip host <R4_Loopback0_IP> host <R2_Loopback0_IP>

route-map PBR permit 10
 match ip address 101
 set ip next-hop <R1_IP_on_10.13.0.0/30>

interface e0/0
 ip policy route-map PBR
```

R4

```
cisco

router ospf 1
 area 1 nssa
```

For Task 1, advertising R3's loopback directly under EIGRP makes it an internal EIGRP route, so R2 prefers it over the OSPF version without changing EIGRP administrative distance.

For Task 2, making Area 1 an NSSA allows redistributed routes to enter the area as Type 7 LSAs while preventing normal Type 5 LSAs from entering it. Redistributing R3's loopback into OSPF on R3 makes that route

visible on R4 through OSPF.
For Task 3, PBR must be applied inbound on R3's interface that receives traffic from R4. The ACL matches traffic from R4 Loopback0 to R2 Loopback0, and the route map forces that traffic to use R1 as the next hop so it always takes the R3-R1 path.

**NEW QUESTION: 248**
How are customer routes isolated on PE routers in an MPLS Layer 3 VPN?
**A.** By using VRF
**B.** By using MP-BGP
**C.** By using LDP
**D.** By using VDCs
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 249**
IPv6 is enabled in the infrastructure to support customers with an IPv6 network over WAN and to connect the head office to branch offices in the local network. One of the customers is already running IPv6 and wants to enable IPv6 over the DMVPN network infrastructure between the headend and branch sites.
Which configuration command must be applied to establish an mGRE IPv6 tunnel neighborship?
**A.** ipv6 nhrp holdtime 30
**B.** tunnel protection mode ipv6
**C.** tunnel mode gre multipoint ipv6
**D.** ipv6 unicast-routing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 250**
Refer to the exhibit. A junior engineer updated a branch router configuration. Immediately after the change, the engineer receives calls from the help desk that branch personnel cannot reach any network destinations.
Which configuration restores service and continues to block 10.1.1.100/32?

```
BRANCH-RTR#

router eigrp 100
 network 10.4.31.0 0.0.0.7
 network 10.100.100.1 0.0.0.0
 distribute-list route-map FILTER-IN in FastEthernet0/0
 eigrp router-id 10.100.100.1
!
ip prefix-list 102 seq 10 permit 10.1.1.100/32
!
route-map FILTER-IN deny 10
 match ip address prefix-list 102
!
```



**A.** route-map FILTER-IN deny 5

**B.** ip prefix-list 102 seq 15 permit 0.0.0.0/32 le 32
**C.** ip prefix-list 102 seq 5 permit 0.0.0.0/32 le 32
**D.** route-map FILTER-IN permit 20
**Answer: (SHOW ANSWER)**
By using "deny" keyword in a route-map, we can filter out the prefix specified in the prefix- list.
But there is an implicit "deny all" statement in the prefix-list so we must permit other prefixes with "permit" keyword in the route-map.

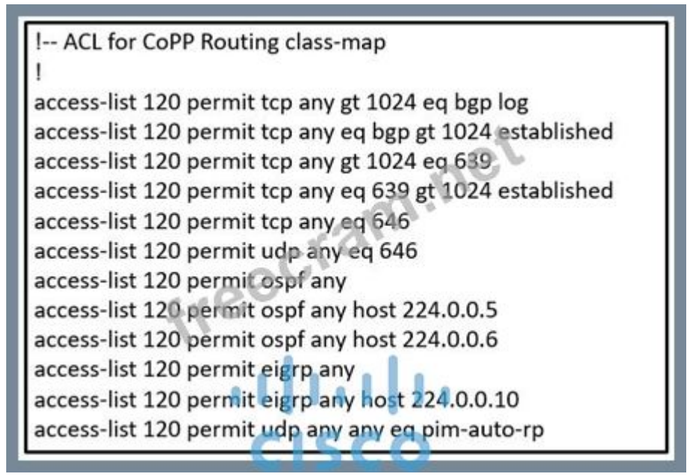
**NEW QUESTION: 251**
Refer to the exhibit. Which statement about R1 is true?

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

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

**A.** RIP learned routes are distributed to OSPF with a tag value of one
**B.** RIP routes are redistributed to OSPF without any changes
**C.** OSPF redistributes RIP routes only if they have a tag of one
**D.** R1 adds one to the metric for RIP learned routes before redistributing to OSPF
**Answer: (SHOW ANSWER)**

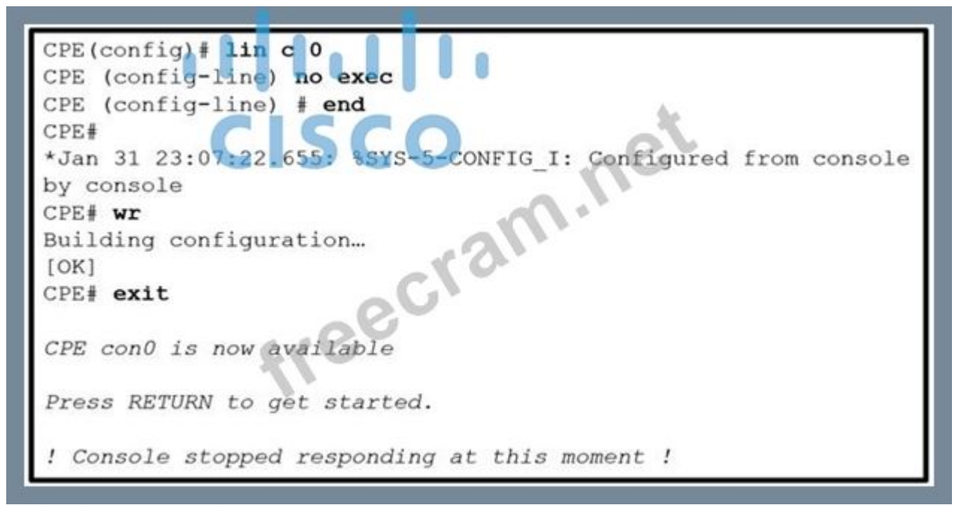
**NEW QUESTION: 252**
An engineer is troubleshooting on the console session of a router and turns on multiple debug commands. The console screen is filled with scrolling debug messages that none of the commands can be verified if entered correctly or display any output.
Which action allows the engineer to see entered console commands while still continuing the analysis of the debug messages?
**A.** Configure the logging synchronous command
**B.** Configure the no logging console debugging command globally
**C.** Configure the logging synchronous level all command
**D.** Configure the term no mon command globally
**Answer: (SHOW ANSWER)**
logging synchronous prevents debug and log messages from interrupting command input on the console. It redisplays the command line after messages appear, allowing the engineer to continue typing and verifying commands while debug output continues.

**NEW QUESTION: 253**
Refer to the exhibit. The control plane is heavily impacted after the CoPP configuration is applied to the router. Which command removal lessens the impact on the control plane?




**A.** access-list 120 permit udp any any eq pim-auto-rp
**B.** access-list 120 permit eigrp any host 224.0.0.10
**C.** access-list 120 permit ospf any
**D.** access-list 120 permit tcp any gt 1024 eq bgp log
**Answer:** (SHOW ANSWER)

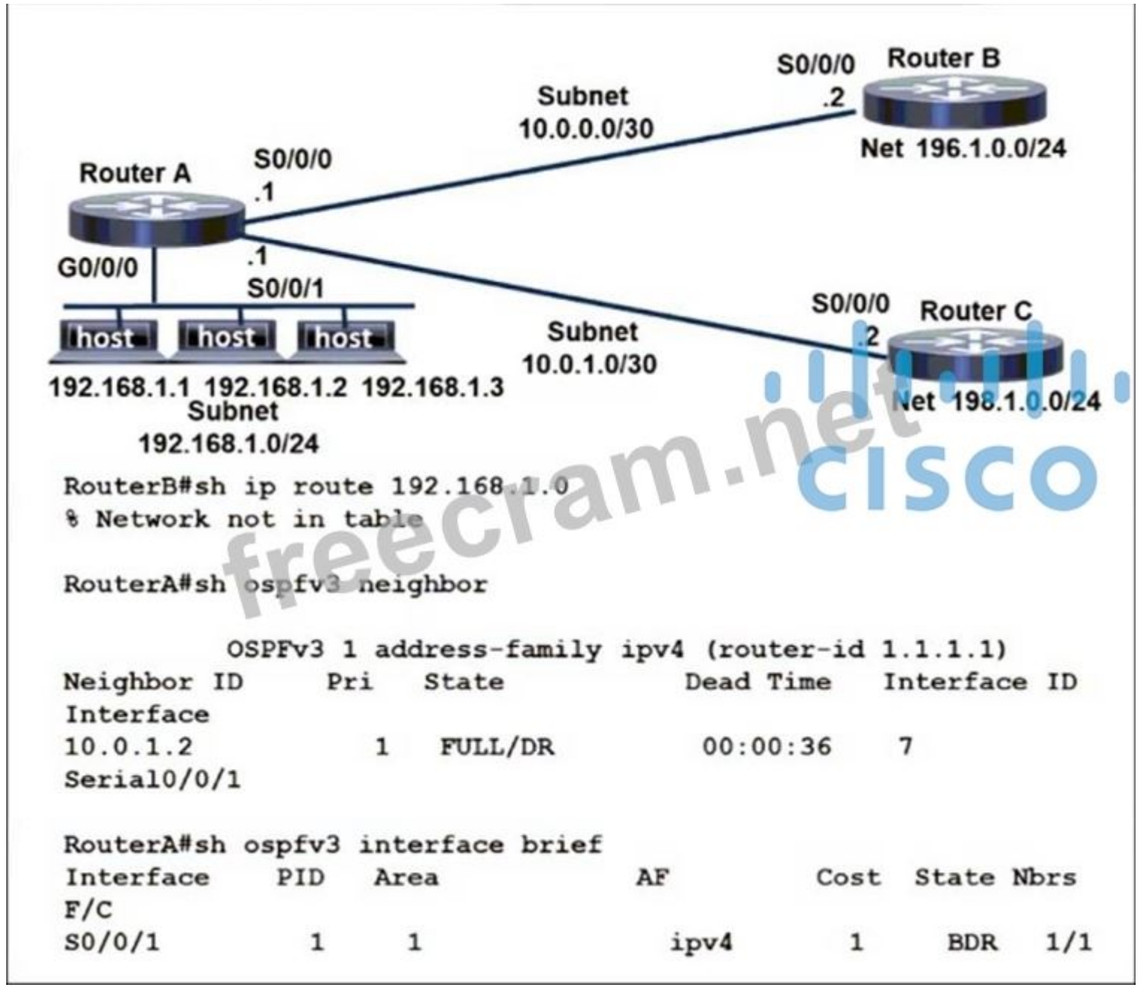
**NEW QUESTION: 254**
Refer to the exhibit. An administrator is attempting to disable the automatic logout after a period of inactivity. After logging out, the console stopped responding to all keyboard inputs. Remote access through SSH still works. Which action resolves the issue?




**A.** Configure the default exec-timeout command on line con 0.
**B.** Configure the no exec-timeout command on line con 0.
**C.** Configure the exec command on line con 0.
**D.** Configure the absolute-timeout command on line con 0.
**Answer:** (SHOW ANSWER)

**NEW QUESTION: 255**

Refer to the exhibit. An engineer must advertise LAN network 192.168.1.0 of router A to router B through OSPF. The engineer notices that router B was configured, but the LAN network of router A is not in the routing table of router B. Which configuration on router A resolves the problem?



A.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

router ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

B.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable

nterface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

'outer ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable

router ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

C.

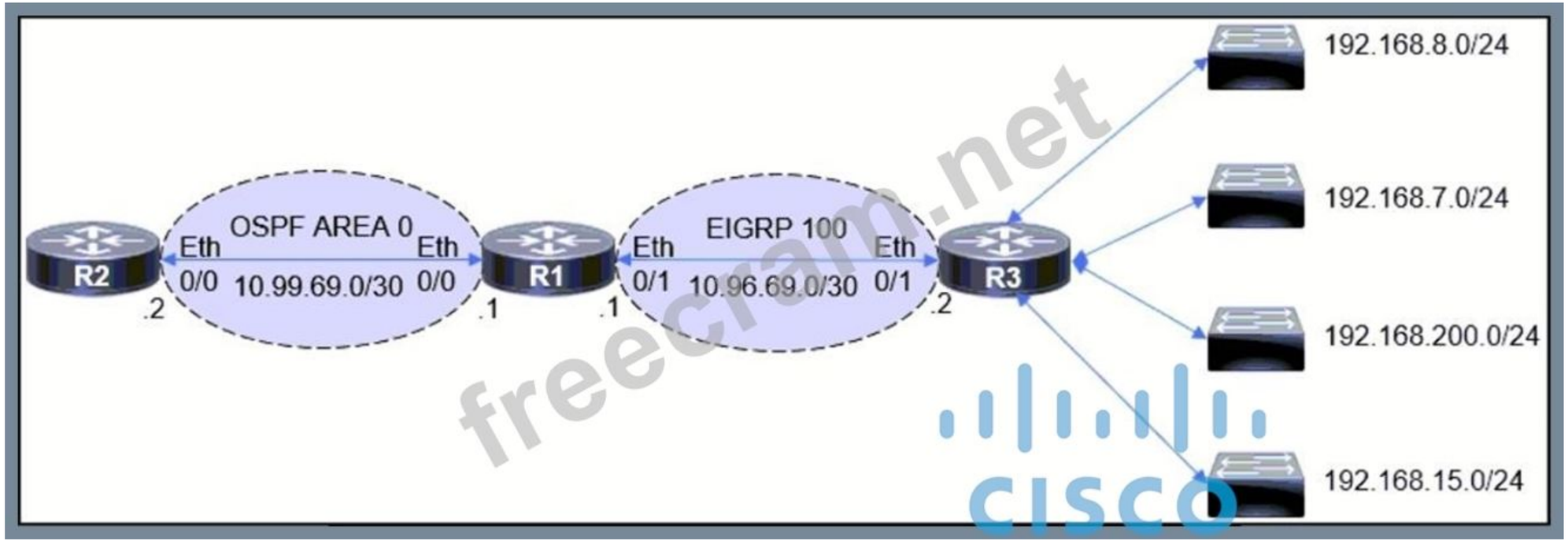
```
interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

router ospfv3 1
 address-family ipv4 unicast
 area 1 range 192.168.1.0 255.255.255.0
 router-id 1.1.1.1
 exit-address-family
```

D.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 256**

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


OSPF AREA 0
Eth 0/0
10.99.69.0/30
Eth 0/0
.2
.1
R2
R1
EIGRP 100
Eth 0/1
10.96.69.0/30
Eth 0/1
.1
.2
R3
192.168.8.0/24
192.168.7.0/24
192.168.200.0/24
192.168.15.0/24
freecram.net
CISCO

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

A.

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

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

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

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

**Answer: (SHOW ANSWER)**



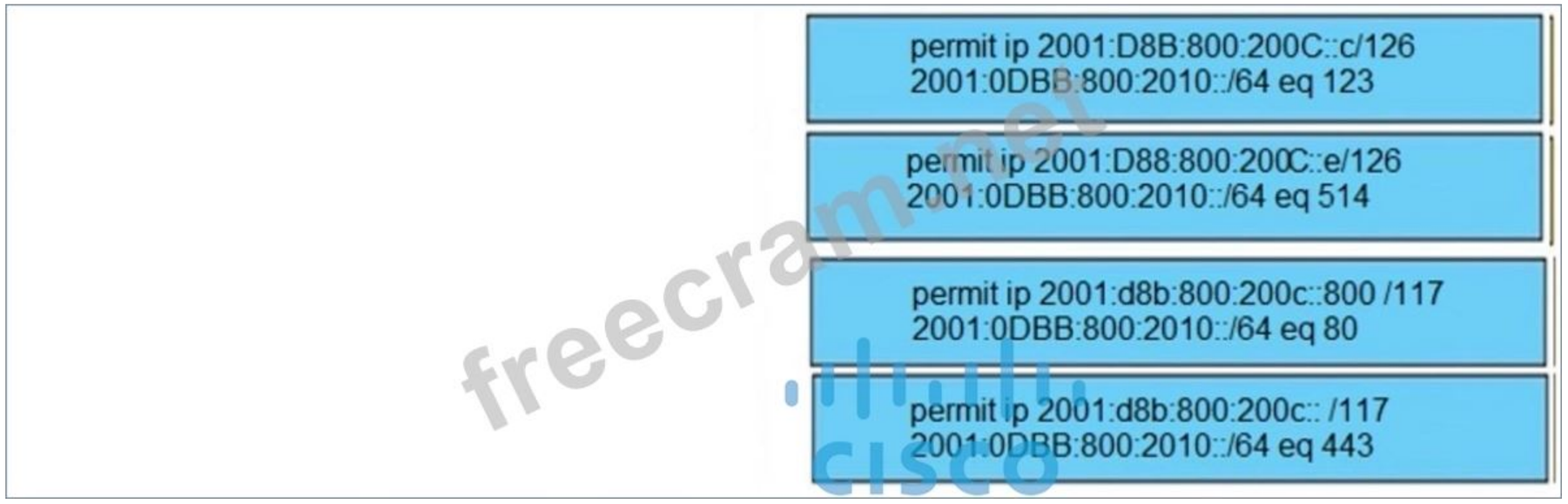
**NEW QUESTION: 257**

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/BootP Relay 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: 258**
Drag and Drop Question
Drag and drop the address from the left onto the correct IPv6 filter purposes on the right.


**Answer:**




Explanation:

HTTP and HTTPs run on TCP port 80 and 443, respectively and we have to remember them.

Syslog runs on UDP port 514 while NTP runs on UDP port 123 so if we remember them we can find out the matching answers easily. But maybe there is some typos in this question as 2001:d88:800:200c::c/126 only ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f (4 hosts in total). It does not cover host 2001:0D88:0800:200c::1f.

Same for 2001:D88:800:200c::e/126, which also ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f and does not cover host 2001:0D88:0800:200c::1c.

**NEW QUESTION: 259**

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)**

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.
+ If the platform ipv6 acl icmp optimize neighbor-discovery command is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.
Reference: 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

**NEW QUESTION: 260**
Refer to the exhibit. an engineer is trying to get 192.168.32.100 forwarded through 10.1.1.1, but it was forwarded through 10.1.1.2. What action forwards the packets through 10.1.1.1?

```
router# show ip route
....
D   192.168.32.0/19 [90/25789217] via 10.1.1.1
R   192.168.32.0/24 [120/4] via 10.1.1.2
O   192.168.32.0/26 [110/229840] via 10.1.1.3
```

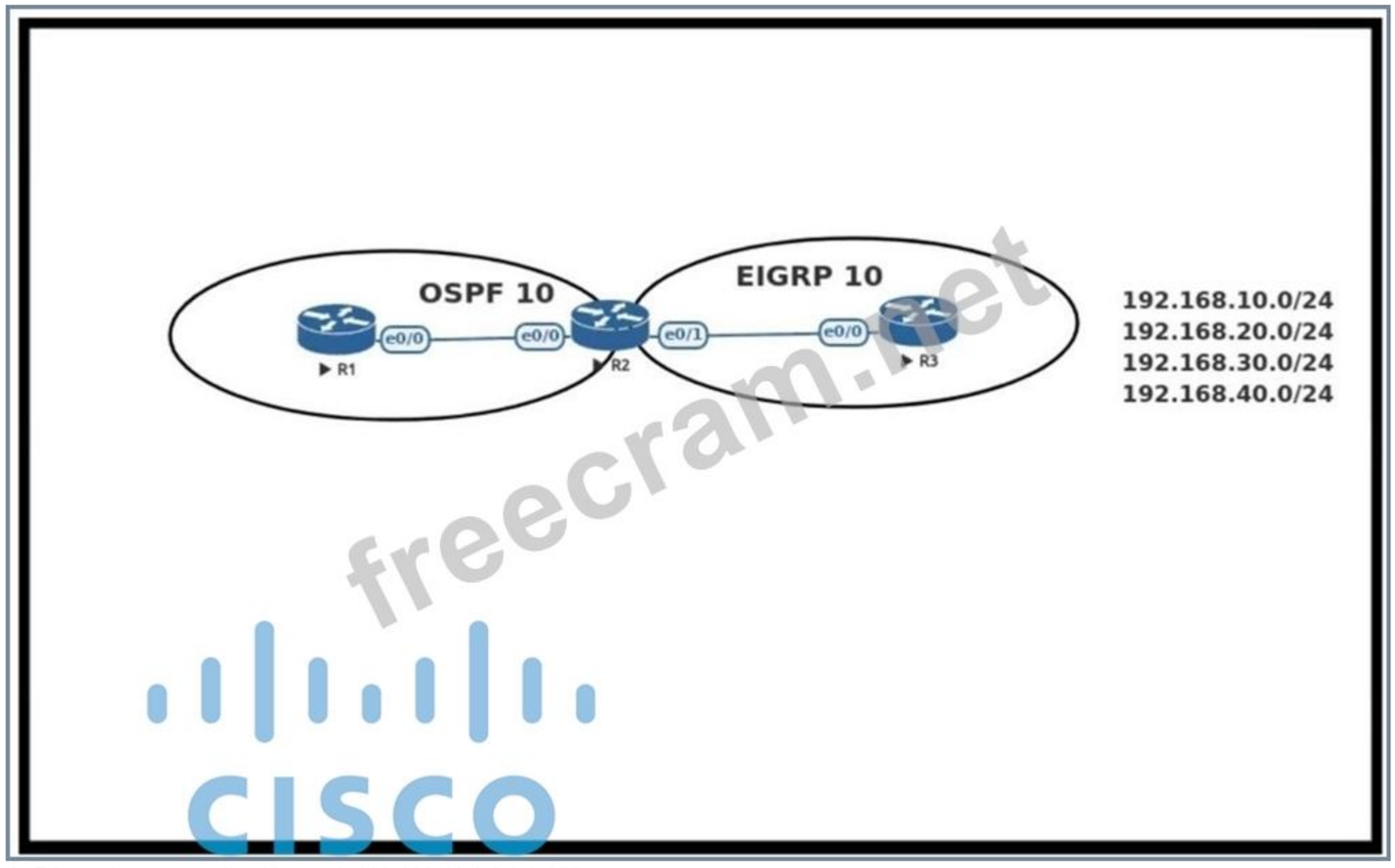
**A.** Configure EIGRP to receive 192.168.32.0 route with lower admin distance.
**B.** Configure EIGRP to receive 192.168.32.0 route with equal or longer prefix than /24.
**C.** Configure EIGRP to receive 192.168.32.0 route with longer prefix than /19.
**D.** Configure EIGRP to receive 192.168.32.0 route with lower metric.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 261**
The network administrator configured the router for Control Plane Policing to limit OSPF traffic to be policed to 1 Mbps.
Any traffic that exceeds this limit must also be allowed at this point for traffic analysis. The router configuration is:

```
access-list 100 permit ospf any any
!
class-map CM-OSPF
 match access-group 100
!
policy-map PM-COPP
 class CM-OSPF
  police 1000000 conform-action transmit
!
control-plane
 service-policy output PM-COPP
```

The Control Plane Policing failed to monitor and police OSPF traffic.
Which configuration resolves this issue?
**A.** policy-map PM-COPP
class CM-OSPF
no police 1000000 conform-action transmit
police 1000000 conform-action transmit exceed-action transmit
!
control-plane
no service-policy output PM-COPP
**B.** policy-map PM-COPP
class CM-OSPF
no police 1000000 conform-action transmit
police 1000000 conform-action transmit
exceed-action transmit
**C.** control-plane
no service-policy output PM-COPP
service-policy input PM-COPP
**D.** no access-list 100
access-list 100 deny ospf any any
access-list 100 permit ip any any
!
policy-map PM-COPP
class CM-OSPF
no police 1000000 conform-action transmit
police 1000000 conform-action transmit exceed-action drop
!
control-plane
no service-policy output PM-COPP
service-policy input PM-COPP
**Answer: A (LEAVE A REPLY)**
Control Plane Policing (CoPP) must be applied correctly for it to take effect. The configuration in the question incorrectly applies the service policy in the output direction instead of the input direction for CoPP, which is designed to manage traffic reaching the control plane.
The corrected configuration includes:
- Removing the service-policy output PM-COPP.
- Applying service-policy input PM-COPP.
Additionally, the exceed-action transmit ensures that excess traffic is still transmitted but monitored for analysis, as per the requirements.

**NEW QUESTION: 262**
Refer to the exhibit. An engineer must redistribute networks 192.168.10.0/24 and
192.168.20.0/24 into OSPF from EIGRP. Where the metric must be added when traversing through multiple hops to start an external route of 20. The engineer notices that the external metric is fixed and does not add at each hop. Which configuration resolves the issue?



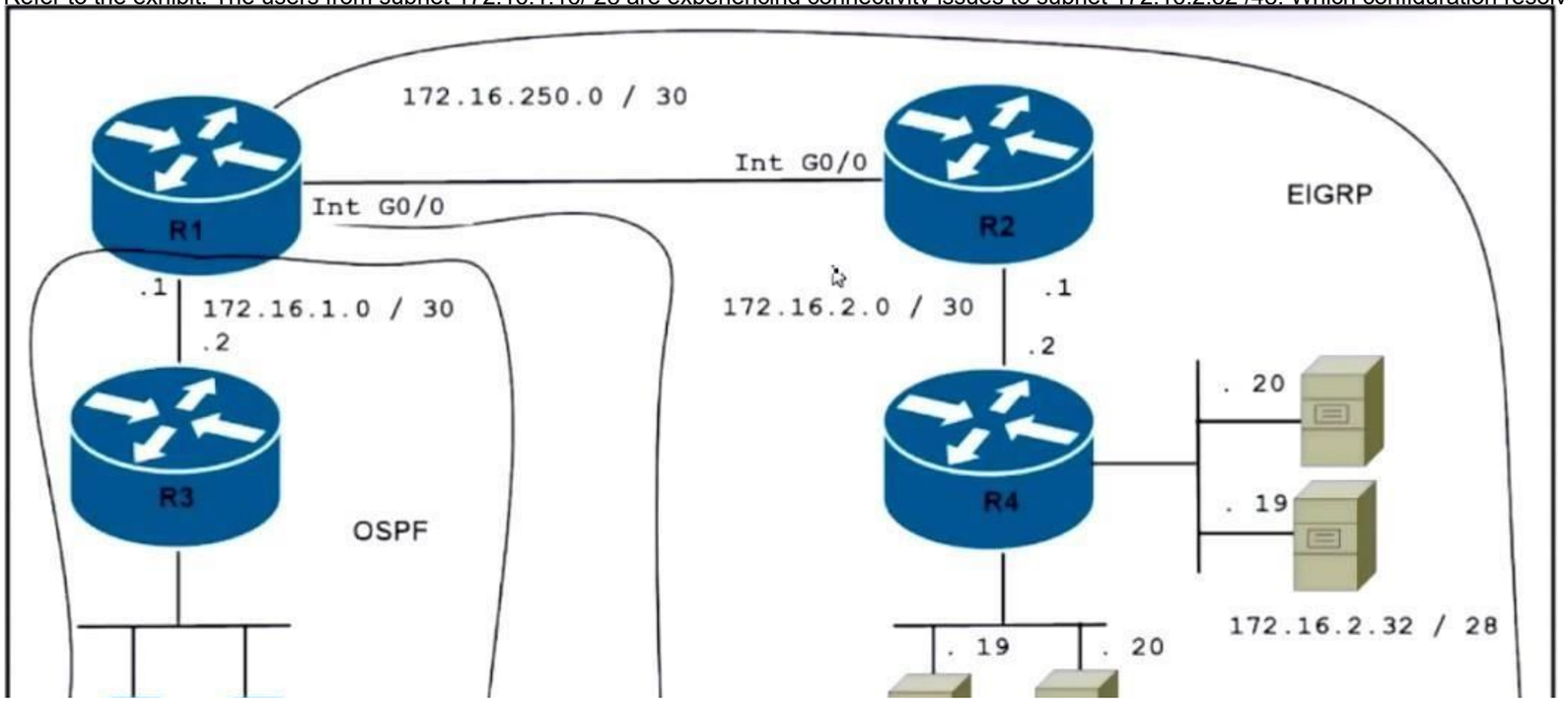



**A.** R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255 !
R2(config)#route-map RD permit 10
R2(config-route-map)#match ip address 10
R2(config-route-map)#set metric 20
R2(config-route-map)#set metric-type type-2 !
R2(config)#router ospf 10
R2(confjg-router)#redistribute eigrp 10 subnets route-map RD

**B.** R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255 !
R2(config)#route-map RD permit 10
R2(config-route-map)#match ip address 10
R2(config-route-map)#set metric 20
R2(config-route-map)#set metric-type type-1 !
R2(config)#router ospf 10

R2(config-router)#redistribute eigrp 10 subnets route-map RD
**C.** R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
(config)#access-list 10 permit 192.168.20.0 0.0.0.255 !
R1(config)#route-map RD permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set metric 20
R1(config-route-map)#set metric-type type-1 !
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 10 subnets route-map RD
**D.** R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255 !
R1(config)#route-map RD permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set metric 20
R1(config-route-map)#set metric-type type-2 !
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 10 subnets route-map RD
**Answer: (SHOW ANSWER)**
Set the route distribution and the metric configuration items to allow the external metric to add to each hop.

**NEW QUESTION: 263**
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?




```
R1#show runn | begin router eigrp 100
router eigrp 100
 network 172.16.250.0 0.0.0.3
 redistribute ospf 10
!
router ospf 10
 redistribute eigrp 100 subnets
 network 172.16.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
```

```
R3#traceroute 172.16.2.17
Type escape sequence to abort.
Tracing the route to 172.16.2.17
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 22 msec 28 msec 13 msec
  2  *  *  *
  3  *  *  *
  4  *  *  *
  5
R3#
```

```
R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 12 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
O E2     172.16.2.0/30 [110/20] via 172.16.1.1, 00:12:20, GigabitEthernet0/1
O E2     172.16.2.16/28 [110/20] via 172.16.1.1, 00:12:20, GigabitEthernet0/1
O E2     172.16.2.32/28 [110/20] via 172.16.1.1, 00:12:20, GigabitEthernet0/1
O E2     172.16.2.48/28 [110/20] via 172.16.1.1, 00:12:20, GigabitEthernet0/1
O E2     172.16.250.0/30 [110/20] via 172.16.1.1, 00:12:20, GigabitEthernet0/
1
R3#
```

```
R4#sho ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set
```

```
      172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C        172.16.2.0/30 is directly connected, GigabitEthernet0/1
L        172.16.2.2/32 is directly connected, GigabitEthernet0/1
C        172.16.2.16/28 is directly connected, Loopback1
L        172.16.2.17/32 is directly connected, Loopback1
C        172.16.2.32/28 is directly connected, Loopback2
L        172.16.2.33/32 is directly connected, Loopback2
S        172.16.2.48/28 [1/0] via 172.16.2.34
D        172.16.250.0/30 [90/3072] via 172.16.2.1, 1d03h, GigabitEthernet0/1
R4#
```

**A.** 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)#redistribute ospf 1 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 ospf 1
R1(config-router)#redistribute eigrp 100 subnets route-map REDIST
**C.** R1(config-router)#router ospf 1
R2(config-router)#redistribute eigrp 100 subnets metric 100
**D.** R1 (config-router)#router eigrp 100
R1(config-router)#redistribute ospf 1 metric 1000000 1 1 1 1
**Answer: (SHOW ANSWER)**
The issue is related to route redistribution between EIGRP and OSPF. Without proper filtering or redistribution rules, certain routes may not be advertised between the routing protocols, resulting in connectivity issues between subnets.
The solution involves:
- Configuring a route-map (REDIST) to control which routes are redistributed from OSPF into EIGRP.
- Applying an access list (access-list 15) to permit only the required subnets (in this case, 172.16.0.0/16).
- Using the route-map during redistribution of OSPF into EIGRP.
Steps in the configuration:
- The access-list ensures only the 172.16.0.0/16 routes are considered.
- The route-map applies this access-list as a match condition.
- The redistribution command ensures these filtered routes are injected into EIGRP with the necessary control.

**NEW QUESTION: 264**
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?

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
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
```

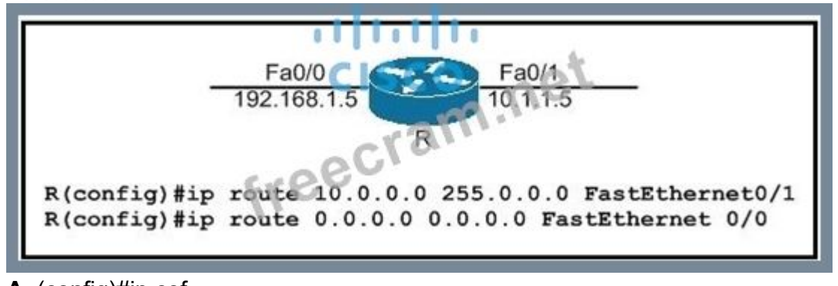
**A.** Configure the debug uptime option.
**B.** Configure the timezone option.
**C.** Configure the log uptime option.
**D.** Configure the msec option.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 265**
What is the downstream unsolicited distribution method in MPLS?
**A.** It sends a unicast hello message to a specific LER.
**B.** It advertises labels to peers only when the peer requests.
**C.** It advertises labels to peers without peer request.
**D.** It sends a unicast hello message to a specific LSR.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 266**
Which of the following are valid restrictions when configuring Control Plane Policing (CoPP) on Cisco devices? (Choose two.)
**A.** The only match types supported with CoPP is ip precedence, ip dscp, and access-group
**B.** CEF must be disabled
**C.** Only standard access-lists are supported.
**D.** You cannot use the "log" keyword with CoPP on the access list entries
**Answer: (SHOW ANSWER)**

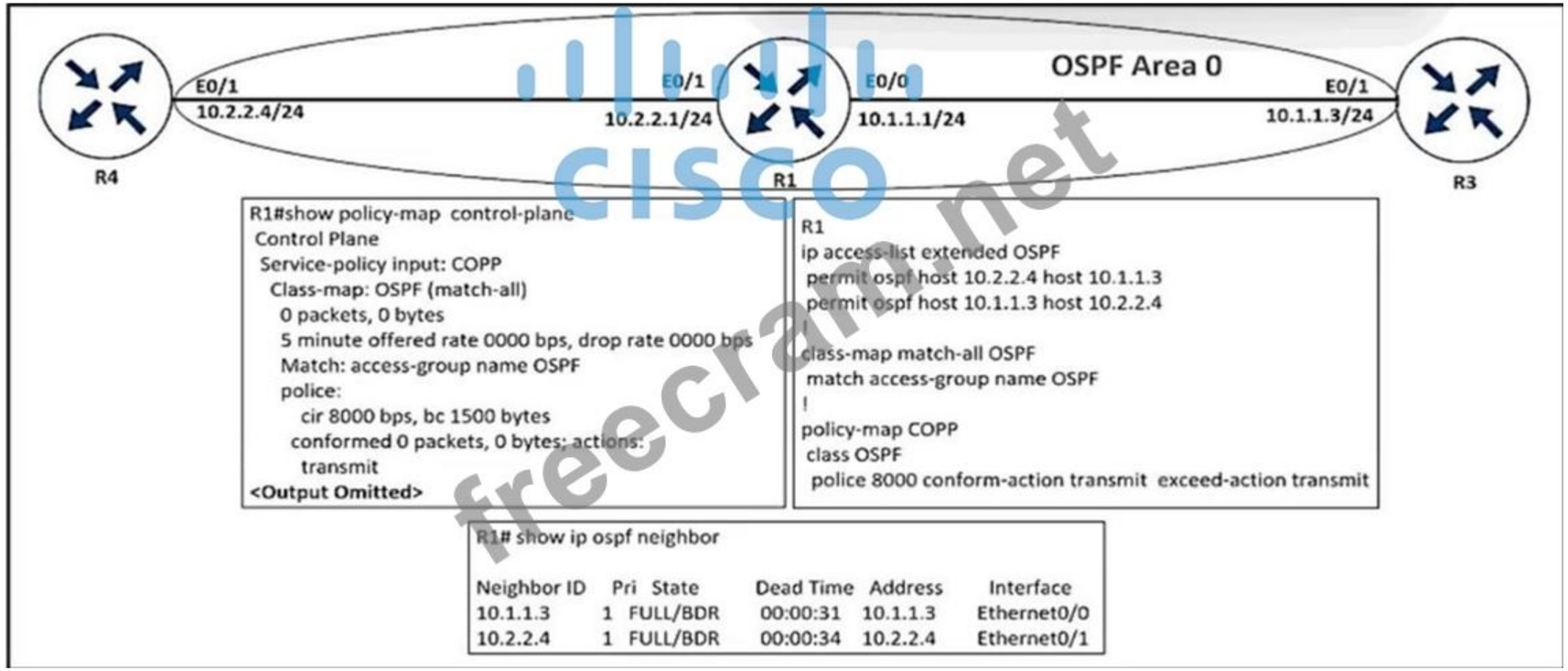
**NEW QUESTION: 267**
Refer to the exhibit. Which option represents the minimal configuration that allows inbound traffic from the 172.16.1.0/24 network to successfully enter router R, while also limiting spoofed

10.0.0.0/8 hosts that could enter router R?




**A.** (config)#ip cef
(config)#interface fa0/0
(config-if)#ip verify unicast source reachable-via rx
**B.** (config)#interface fa0/0
(config-if)#ip verify unicast source reachable-via any
**C.** (config)#ip cef
(config)#interface fa0/0
(config-if)#ip verify unicast source reachable-via rx allow-default
**D.** (config)#no ip cef
(config)#interface fa0/0
(config-if)#ip verify unicast source reachable-via rx
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 268**
Refer to the exhibit. An engineer implemented CoPP but did not see OSPF traffic going through it.
Which configuration resolves the issue?






**A.** ip access-list extended OSFP
permit ospf any any
**B.** policy-map COPP
class OSFP
police 8000 conform-action transmit exceed-action transmit violate-action drop
**C.** class-map match-all OSFP
match access-group name OSFP
**D.** control-plane
service-policy input COPP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 269**
Refer to the exhibit. When monitoring an IPv6 access list, an engineer notices that the ACL does not have any hits and is causing unnecessary traffic to pass through the interface. Which command must be configured to resolve the issue?

```
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
```

**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: 270**
Refer to the exhibit. R1 is being monitored using SNMP and monitoring devices are getting only partial information. What action should be taken to resolve this issue?

```
R1#show policy-map control-plane
  Control Plane
        Service-policy output: CoPP
         Class-map: SNMP-Out (match-all)
           124 packets, 3693 bytes
           5 minute offered rate 0000 bps, drop rate 0000 bps
           Match: access-group name SNMP
           police:
                cir 8000 bps, bc 1500 bytes
              conformed 0 packets, 0 bytes; actions:
                transmit
              exceeded 0 packets, 0 bytes; actions:
                drop
              conformed 0000 bps, exceeded 0000 bps

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

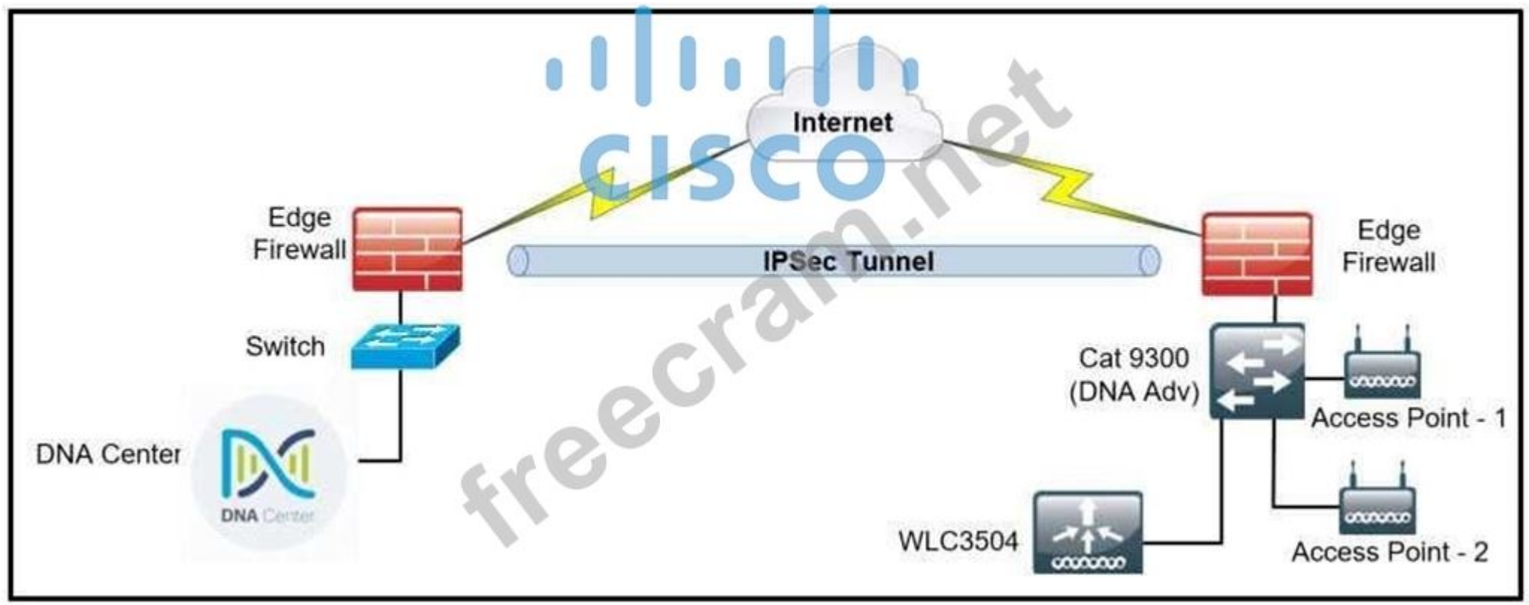


**A.** Modify the CoPP policy to increase the configured exceeded limit for SNMP.
**B.** Modify the access list to include snmptrap.
**C.** Modify the CoPP policy to increase the configured CIR limit for SNMP.
**D.** Modify the access list to add a second line to allow udp any any eq snmp.

**Answer: (SHOW ANSWER)**

From the output we can see no SNMP packets have been drop so far so we don't need to increase any SNMP limitation. The following statement should be added to the ACL: "permit udp any any eq snmptrap" so that additional information can be sent.

**NEW QUESTION: 271**
Refer to the exhibit. A network administrator is discovering a Cisco Catalyst 9300 and a Cisco WLC 3504 in Cisco DNA Center. The Catalyst 9300 is added successfully However the WLC is showing [ error "uncontactable" when the administrator tries to add it in Cisco DNA Center.
Which action discovers WLC in Cisco DNA Center successfully?




**A.** Copy the .cert file from the Cisco DNA Center on the USB and upload it to the WLC 3504.
**B.** Delete the WLC 3504 from Cisco DNA Center and add it to Cisco DNA Center again.
**C.** Add the WLC 3504 under the hierarchy of the Catalyst 9300 connected devices.
**D.** Copy the .pern file from the Cisco DNA Center on the USB and upload it to the WLC 3504.
**Answer: (SHOW ANSWER)**
Cisco DNA Center requires secure HTTPS communication with devices. The WLC must trust the DNA Center certificate to allow communication. Uploading the .pem certificate from DNA Center to the WLC establishes trust and resolves the "uncontactable" status.



**NEW QUESTION: 272**
The network administrator deployed the Binding Table Recovery feature. Which two devices recover the missing binding table entries? (Choose two.)
**A.** DHCP client
**B.** destination host
**D.** source host
**C.** DHCP relay agent
**E.** DHCP server

**Answer: (SHOW ANSWER)**

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. Upon a failure, a binding table entry is recovered by querying the DHCP server or the destination host depending on the configuration.

**NEW QUESTION: 273**

Refer to the exhibit. An engineer must filter prefixes that originate from AS65412, but it is not working correctly. Which configuration must the engineer apply to R1 to resolve the issue?

R1

```
ip as-path access-list 1 deny 65412_$
ip as-path access-list 1 permit .*

router bgp 64560
   neighbor 10.10.10.10 remote-as 64570
   neighbor 10.10.10.10 route-map FILTER in

route-map FILTER permit 10
   match as-path 1

R1#show ip bgp
```

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|---|---|---|---|---|---|
| *> 10.0.0.0/8 | 10.10.10.10 | 0 | 100 | 0 | 64570 i |
| *> 10.1.0.0/16 | 10.10.10.10 | 0 | 100 | 0 | 64570 i |
| *> 10.1.1.0/24 | 10.10.10.10 | 0 | 100 | 0 | 64570 65412 i |
| *> 10.1.2.0/24 | 10.10.10.10 | 0 | 100 | 0 | 64570 65412 i |
| *> 10.1.3.0/24 | 10.10.10.10 | 0 | 100 | 0 | 64570 65412 i |
| *> 10.1.4.0/24 | 10.10.10.10 | 0 | 100 | 0 | 64570 65412 i |
| *> 10.1.5.0/24 | 10.10.10.10 | 0 | 100 | 0 | 64570 65412 i |
| *> 10.1.6.0/24 | 10.10.10.10 | 0 | 100 | 0 | 64570 65412 i |

**A.** no ip as-path access-list 1
ip as-path access-list 1 deny _65412$
ip as-path access-list 1 permit .*
**B.** route-map FILTER permit 10
match as-path 1

route-map FILTER permit 20
**C.** no ip as-path access-list 1
ip as-path access-list 1 deny 65412_
ip as-path access-list 1 permit.*
**D.** router bgp 64560
neighbor 10.10.10.10 route-map FILTER out
**Answer: (SHOW ANSWER)**
The issue lies in the existing AS-path access list configuration. The current access list uses the regular expression 65412$, which matches any AS-path that ends with 65412. However, this does not account for AS-paths where AS 65412 appears anywhere except the last position.
The regex _65412$ is used instead of 65412$. The underscore _ ensures a match only when AS
65412 is a complete AS number (not part of a larger number) and occurs at the end of the AS- path. The access list must be updated with the new regex to filter routes originating from AS
65412 correctly.

**NEW QUESTION: 274**
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 ignore
**B.** ip nhrp registration no-registration
**C.** ip nhrp registration dynamic
**D.** ip nhrp registration no-unique
**Answer: (SHOW ANSWER)**
Non-Unique Registrations
If you're experiencing DMVPN downtime due to changing public IP addresses of your DMVPN spokes, apply the ip nhrp registration non-unique interface configuration command to the DMVPN tunnel interface. This command will reduce the recovery time to less than a minute. Faster recovery is harder to achieve as the router has to execute a number of steps following a physical interface flap:
Install new static routes to the hub sites;
Create IPSec session with the hub sites;
Register new public IP address with NHRP;
Establish routing adjacency.
You can fine-tune steps 1-3 on the spoke router; step 4 sometime requires coordinated changes throughout the network.

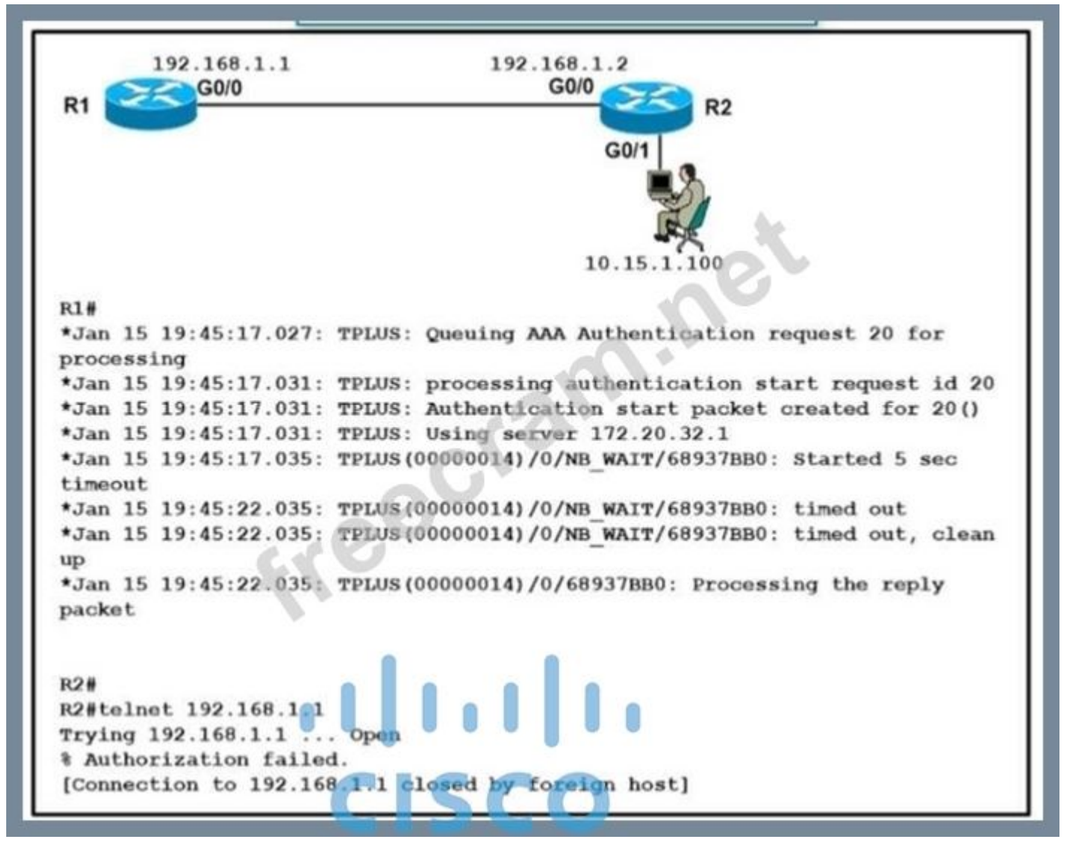
**NEW QUESTION: 275**
Which of the following statements are true regarding two OSPF routers to become neighbors?
(Choose two.)
**A.** Must have matching MTU's on the physical network links that connect the routers.
**B.** Need not be on the same subnet.
**C.** Must have identical hello and dead timers
**D.** Must use the same ASN
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 276**
Refer to the exhibit. After a new regional office is set up, not all guests can access the internet via guest Wi Fi. Clients are getting the correct IP address from guest Wi-Fi VLAN 364.

Which action resolves the issue ?

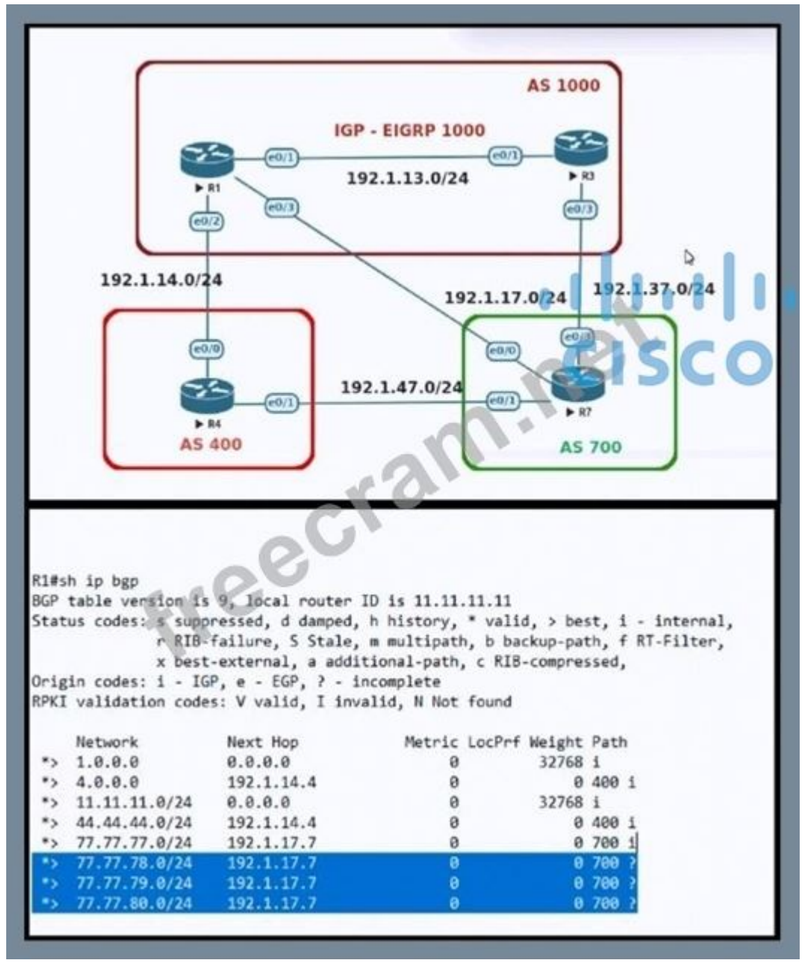

**A.** Allow DNS traffic through the inbound ACL
**B.** Allow 10.66.46.0/23 in the inbound ACL
**C.** Allow DNS traffic through the outbound ACL
**D.** Allow 10.66.46.0/23 in the outbound ACL
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 277**
Refer to the exhibit. A network engineer is troubleshooting an AAA authentication issue for R1 from R2. When an engineer tries to open a telnet connection to R1 it opens the connection but shows a %Authorization failed error message on the terminal and closes the connection silently.
Which action resolves the issue?




**A.** Resolve tacacs+ server host IP authentication miss configuration on the R1 router
**B.** Resolve tacacs+ server reachability from the R1 router.
**C.** Configure the tacacs+ server host IP on the R1 router
**D.** Configure authorization commands in the tacacs* server for the R1 router.
**Answer: (SHOW ANSWER)**

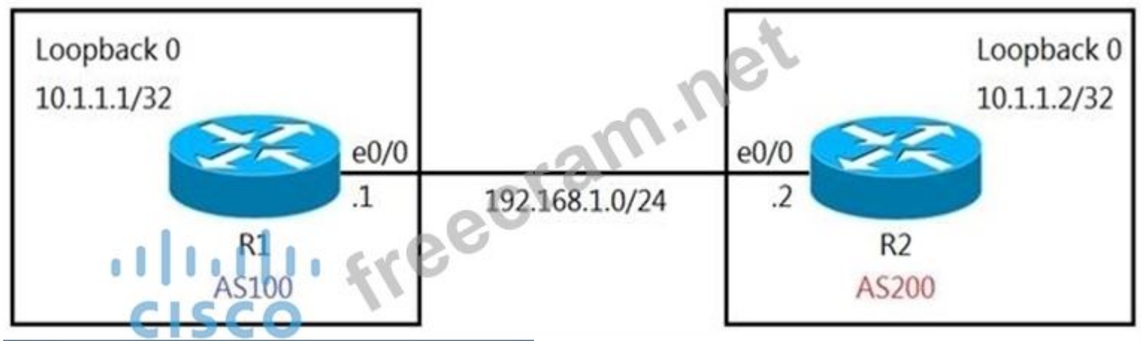
**NEW QUESTION: 278**
Refer to the exhibit. R1 should have BGP routes as "i". Which configuration resolves the issue?




**A.** R7
route-map RC permit 10
match ip address 1
set origin igp
**B.** R7
route-map RC permit 10
match ip address 1
set metric 1
**C.** R1
route-map RC permit 10
match ip address 1
set origin igp
**D.** R1
route-map RC permit 10

match ip address 1
set metric 1
**Answer: (SHOW ANSWER)**
The origin code in BGP indicates where a route originated from. By default, when a route is injected into BGP using the network command, the origin code is i (IGP). If the origin is set to something else (e.g., incomplete), the BGP attributes may not behave as expected.
In this case, to ensure that R1 receives the routes from R7 with the origin code as i, a route-map needs to be applied on R7 to modify the origin attribute for the specified routes. The set origin igp command in the route-map modifies the origin code for the routes matched by the access list.

**NEW QUESTION: 279**
Refer to the exhibit. The R1 and R2 configurations are:




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

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

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

**A.**

```
R1

ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
 neighbor 10.1.1.1 ttl-security hops 1
 neighbor 10.1.1.2 update-source loopback 0
```

B.

```
R2

ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
 neighbor 10.1.1.2 ttl-security hops 1
 neighbor 10.1.1.2 update-source loopback 0
```

C.

```
R2

ip route 10.1.1.1 255.255.255.255 192.168.1.1
!
router bgp 200
neighbor 10.1.1.1 ttl-security hops 1
neighbor 10.1.1.1 update-source loopback 0
```

D.

```
R1

ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
 neighbor 10.1.1.2 disable-connected-check
 neighbor 10.1.1.2 update-source Loopback0
```

**E.**

```
R2

ip route 10.1.1.1 255.255.255.255 192.168.1.1
!
router bgp 200
 neighbor 10.1.1.1 disable-connected-check
 neighbor 10.1.1.1 update-source loopback 0
```

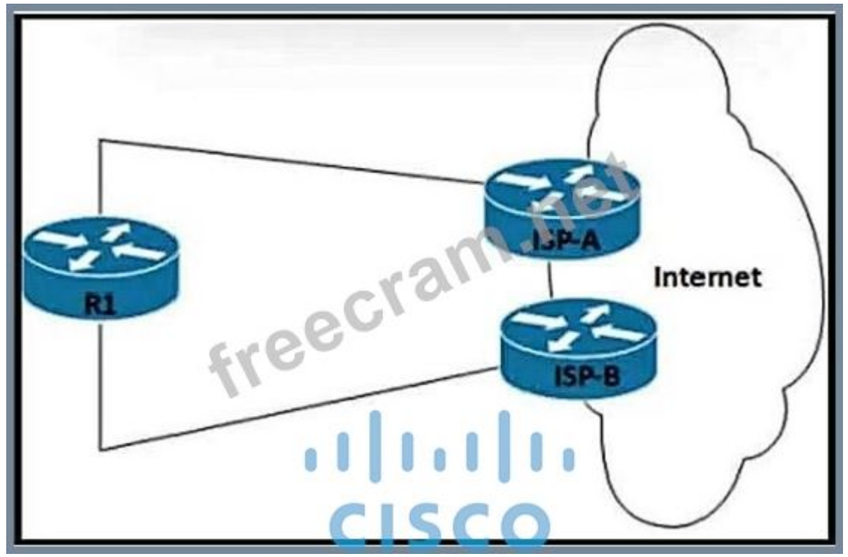
**Answer: D,E (LEAVE A REPLY)**

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.

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.

**NEW QUESTION: 280**

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

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

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

**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)**
https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/floating-static-route If we want to use a static route as a backup route, we'll have to change its administrative distance. This is called a floating static route.
https://www.geeksforgeeks.org/what-is-floating-static-route/
higher admin value to make a secondary route:
Router(config)#ip route 192.168.60.0 255.255.255.0 192.168.40.2 (primary route) Router(config)#ip route 192.168.60.0 255.255.255.0 192.168.20.2 10 (secondary route)

**NEW QUESTION: 281**
What is the failure detection time with BFD?
**A.** less than a second
**B.** 3 seconds
**C.** 2 seconds
**D.** 1 second
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 282**
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?

```
Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
  Advertised to update-groups:
     1         2         3
(65001 64955 65003) 65089, (Received from a RR-client)
  172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
    Origin IGP, metric 0, localpref 100, valid, confed-internal
    Extended Community: RT:1100:1001
    mpls labels in/out 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-internal
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-internal
Extended Community: RT:1100:1001
mpls labels in/out nolabel/278

**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)**
By adding extra AS_PATH makes the current best-path #6 less preferred compared to route #5.

**NEW QUESTION: 283**
Routers R1 and R2 have been configured to use Bidirectional Forwarding Detection? What is the advantage of doing this?
**A.** It is able to discover local link failures at layers 1 and 2 and provides detection for this in less than one second.
**B.** It is able to discover local link failures at layer 1 and provide automatic re-routing
**C.** It is able to discover local link failures at layer 1 only and provides detection for this in less than one second.
**D.** It is able to discover local link failures at layer 1 and provide automatic re-routing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 284**

Refer to the exhibit. A network administrator configured an IPv6 access list to allow TCP return traffic only, but it is not working as expected. Which changes resolve this issue?

```
ipv6 access-list inbound
 permit tcp any any
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound out
```

A.

```
ipv6 access-list inbound
 permit tcp any any established
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound in
```

B.

```
ipv6 access-list inbound
 permit tcp any any established
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound out
```

C.

```
ipv6 access-list inbound
 permit tcp any any syn
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound in
```

```
ipv6 access-list inbound
 permit tcp any any syn
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound out
```

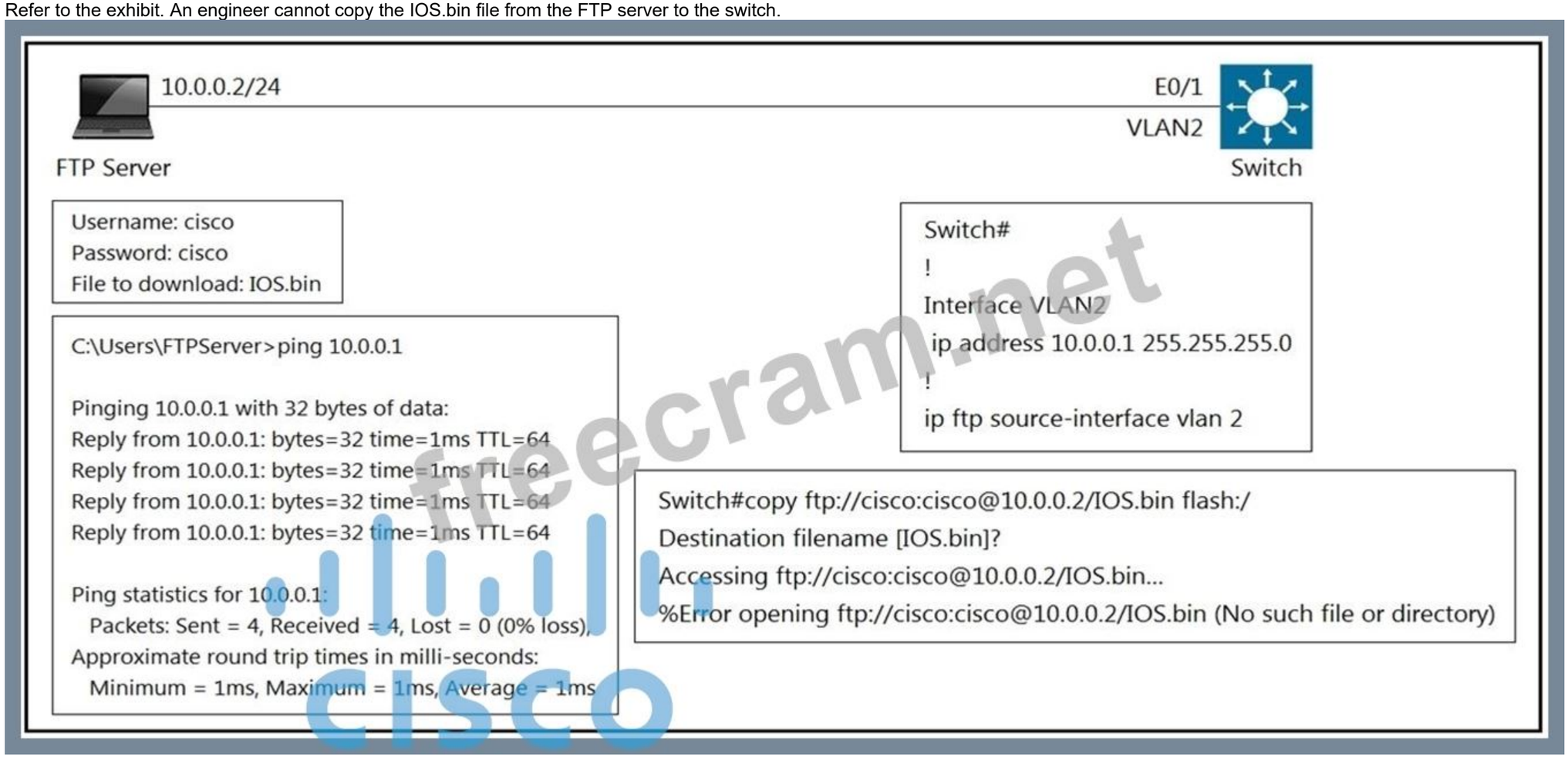
**D.**

**Answer: (SHOW ANSWER)**

To allow only return TCP traffic, the ACL must use the established keyword so only packets with the ACK or RST bits set are permitted. Additionally, the ACL must be applied in the inbound direction to filter incoming traffic correctly.

**NEW QUESTION: 285**

Refer to the exhibit. An engineer cannot copy the IOS.bin file from the FTP server to the switch.



Which action resolves the issue?

**A.** Allow file permissions to download the file from the FTP server.

**B.** Use the copy flash:/ ftp://cisco@10.0.0.2/IOS.bin command.

**C.** Make memory space on the switch flash or USB drive to download the file.

**D.** Add the IOS.bin file, which does not exist on FTP server.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 286**

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?

**Debug output:**

```
username: USER55
password:
Aug 26 12:39:23.812: TPLUS: Queuing AAA Authentication request 4950 for processing
Aug 26 12:39:23.812: TPLUS(00001356) login timer started 1020 sec timeout
Aug 26 12:39:23.812: TPLUS: processing authentication continue request id 4950
Aug 26 12:39:23.812: TPLUS: Authentication continue packet generated for 4950
Aug 26 12:39:23.812: TPLUS(00001356)/0/WRITE/3A72C8D0: Started 5 sec timeout
!
!----- output omitted -----!
!
Aug 26 12:40:01.241: TAC+: using previously set server 192.168.1.3 from group tacacs+
Aug 26 12:40:01.241: TAC+: Opening TCP/IP to 192.168.1.3/49 timeout=5
Aug 26 12:40:01.249: TAC+: Opened TCP/IP handle 0x3BE31D1C to 192.168.1.3/49
Aug 26 12:40:01.249: TAC+: Opened 192.168.1.3 index=1
Aug 26 12:40:01.250: TAC+: 192.168.1.3 (3653537180) AUTOR/START queued
Aug 26 12:40:01.449: TAC+: (3653537180) AUTOR/START processed
Aug 26 12:40:01.449: TAC+: (-641430116): received author response status = FAIL
Aug 26 12:40:01.450: TAC+: Closing TCP/IP 0x3BE31D1C  connection to 192.168.1.3/49
```

**A.** Configure full access for the username from TACACS+ server

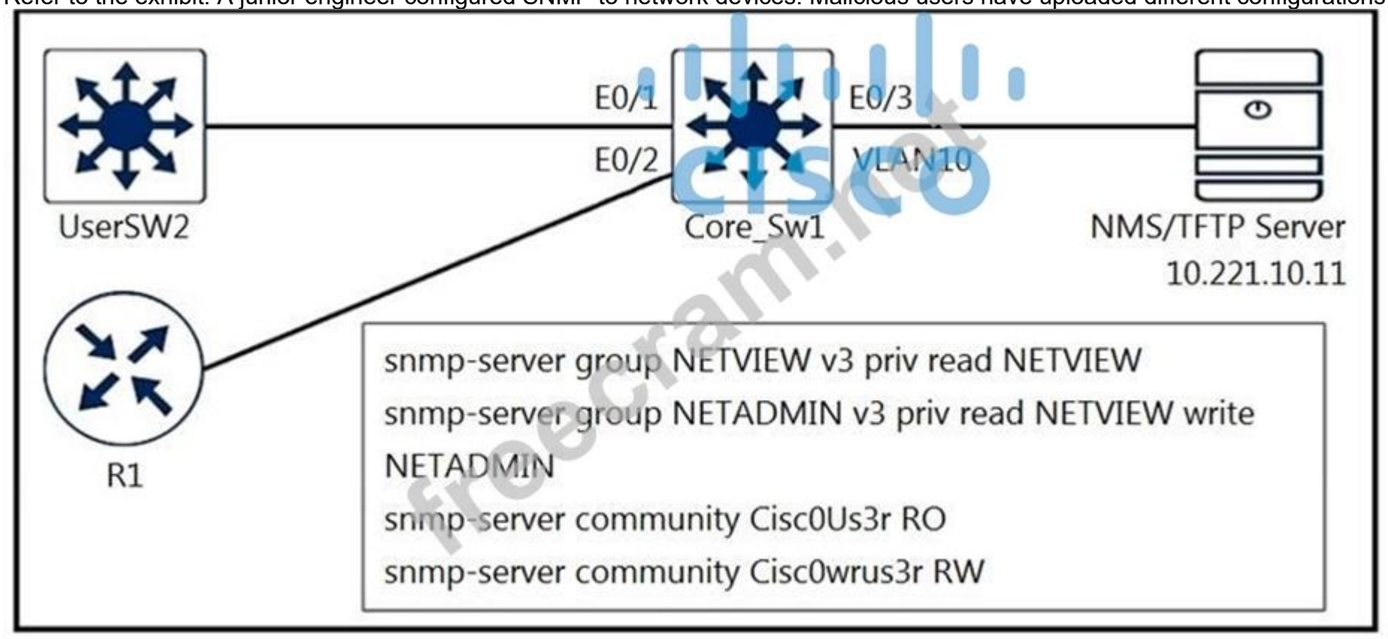
**B.** Configure the username from a local database

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

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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 287**
Refer to the exhibit. A junior engineer configured SNMP to network devices. Malicious users have uploaded different configurations to the network devices using SNMP and TFTP servers.




Which configuration prevents changes from unauthorized NMS and TFTP servers?
**A.** access-list 20 permit 10.221.10.11
**B.** access-list 20 permit 10.221.10.11
access-list 20 deny any log
!
snmp-server group NETVIEW v3 priv read NETVIEW access 20
snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20 snmp-server community Cisc0wrus3r RO 20 snmp-server community Cisc0Us3r RW 20 snmp-server tftp-server-list 20
**C.** access-list 20 permit 10.221.10.11
access-list 20 deny any log
!
snmp-server group NETVIEW v3 priv read NETVIEW access 20
snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20 snmp-server community Cisc0Us3r RO 20 snmp-server community Cisc0wrus3r RW 20 snmp-server tftp-server-list 20
**D.** access-list 20 permit 10.221.10.11
access-list 20 deny any log
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 288**

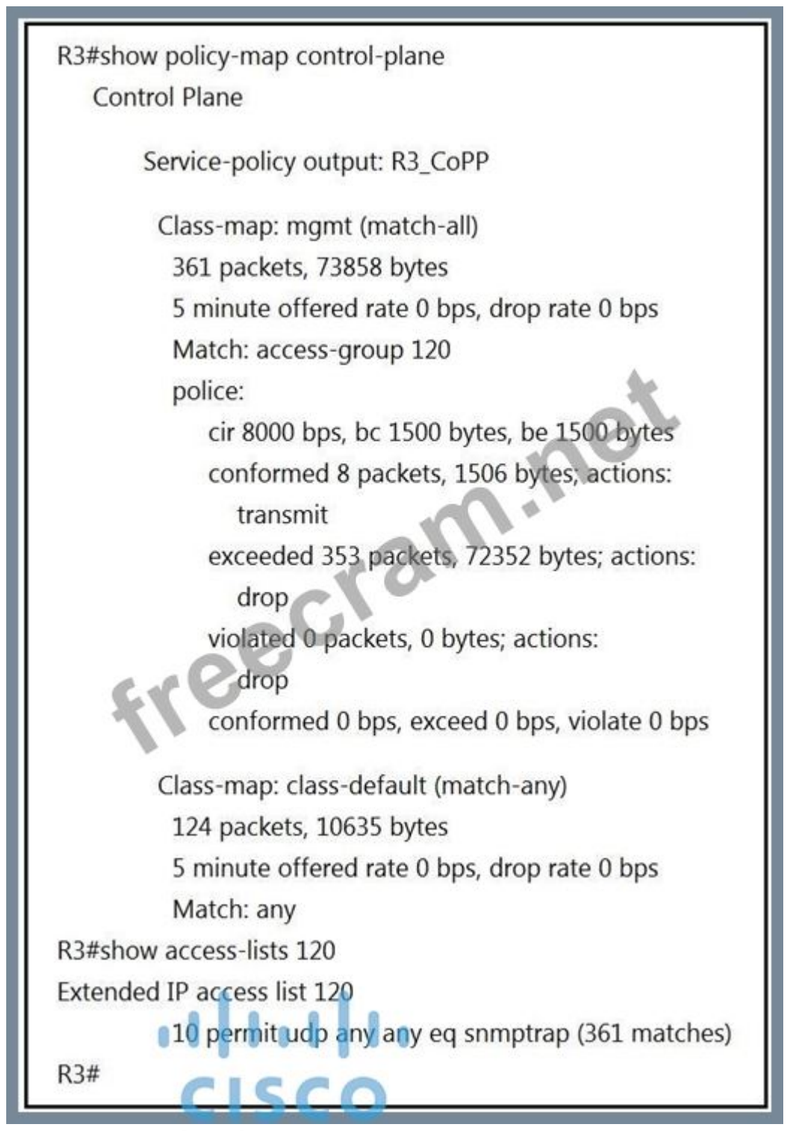
Refer to the exhibit. The BGP neighbor is not coming up. Which action resolves the issue?

```
R1
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.200.6 remote-as 100
 neighbor 192.168.200.6 update-source Loopback0
 no auto-summary
!
ip route 192.168.200.6 255.255.255.255 192.168.100.1
!
R1#show ip bgp neighbor 192.168.200.6
BGP neighbor is 192.168.200.6,  remote AS 100, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 00:00:00, last write 00:00:00, hold time is 180, keepalive interval is
  60 seconds
!
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0/0
  Output queue size: 0
  Index 1, Offset 0, Mask 0x2
  !
  Connections established 0; dropped 0
  Last reset never
  No active TCP connection
```

**A.** Configure the ebgp-multihop 2 command on R1 toward the neighbor.
**B.** Configure a valid router ID on the neighbor that shows an invalid router ID of 0.0.0.0.
**C.** The route map on eBGP sessions must allow the prefixes from the neighbor.
**D.** Enable synchronization between the neighbors to bring the neighborship up.
**Answer: (SHOW ANSWER)**
eBGP (external BGP) by default requires two Cisco IOS routers to be directly connected to each other in order to establish a neighbor adjacency. This is because eBGP routers use a TTL of one for their BGP packets. When the BGP neighbor is more than one hop away, the TTL will decrement to 0 and it will be discarded.
When these two routers are not directly connected then we can still make it work but we'll have to use multihop. This requirement does not apply to internal BGP. This is the case in this example since we have configured the update source to tbe the loopback0 interface, not the physical interface connecting these two routers together.

**NEW QUESTION: 289**
Which of the following are valid TFTP error codes? (Choose two.)
**A.** Error code 8 - Undefined error
**B.** Error Code 1 - File not found
**C.** Error code 6 - File already exists
**D.** Error Code 2 - Unknown error
**E.** Error code 3 - Invalid user
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 290**
Refer the exhibit. Which action resolves intermittent connectivity observed with the SNMP trap packets?

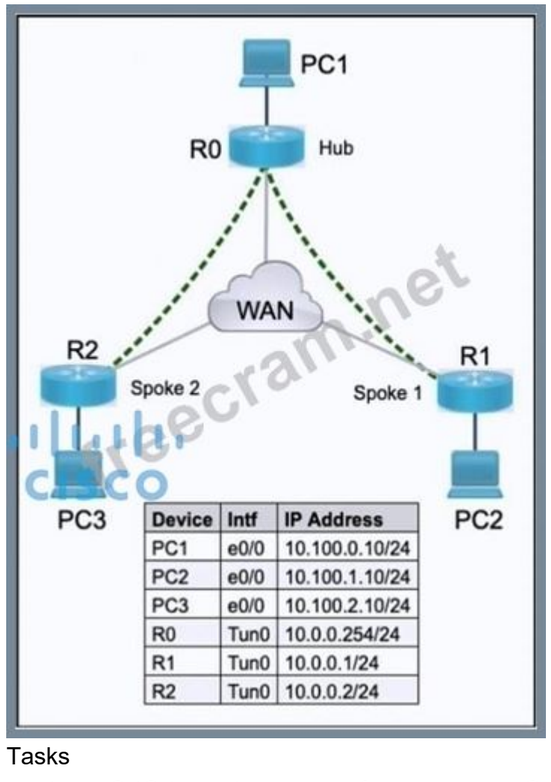



**A.** Increase the CIR of the mgmt class map
**B.** Decrease the committed burst Size of the mgmt class map
**C.** Add a new class map to match TCP traffic
**D.** Add one new entry in the ACL 120 to permit the UDP port 161
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 291**
An engineer is creating a policy that overrides normal routing behavior. If the route to a destination of 10.100.100.0/24 is withdrawn from the routing table, the policy must direct traffic to a next-hop of 10 .1.1.1. If the route is present in the routing table, then normal forwarding must occur. Which configuration meets the requirements?
**A.** access-list 100 permit ip any any

!
route-map POLICY permit 10
match ip address 100
set ip next-hop recursive 10.1.1.1
**B.** access-list 100 permit ip any 10.100.100.0 0.0.0.255
!
route-map POLICY permit 10
match ip address 100
set ip default next-hop 10.1.1.1
**C.** access-list 100 permit ip any 10.100.100.0 0.0.0.255
!
route-map POLICY permit 10
match ip address 100
set ip next-hop 10.1.1.1
!
route map POLICY permit 20
**D.** access-list 100 permit ip any 10.100.100.0 0.0.0.255
!
route map POLICY permit 10
match ip address 100
set ip next-hop recursive 10.1.1.1
!
route-map POLICY permit 20
**Answer: (SHOW ANSWER)**
set ip default next-hop applies policy-based routing only when there is no matching route for the destination in the routing table. That matches the requirement to use 10.1.1.1 only when 10.100.100.0/24 is no longer present, while allowing normal forwarding whenever the route exists.

**NEW QUESTION: 292**
LAB SIMULATION 13
Guidelines
This is a lab item in which tasks will be performed on virtual devices.
* Refer to the Tasks tab to view the tasks for this lab item.
* Refer to the Topology tab to access the device console(s) and perform the tasks.
* Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
* All necessary preconfigurations have been applied.
* Do not change the enable password or hostname for any device.
* Do not replace existing routing policies or configurations.
* Save your configurations to NVRAM before moving to the next item.
* Click Next at the bottom of the screen to submit this lab and move to the next question.
* When Next is clicked, the lab closes and cannot be reopened.
Topology




| Device | Intf | IP Address |
|---|---|---|
| PC1 | e0/0 | 10.100.0.10/24 |
| PC2 | e0/0 | 10.100.1.10/24 |
| PC3 | e0/0 | 10.100.2.10/24 |
| R0 | Tun0 | 10.0.0.254/24 |
| R1 | Tun0 | 10.0.0.1/24 |
| R2 | Tun0 | 10.0.0.2/24 |

Tasks

HUB and SPOKE routers are configured using mGRE tunnels according to the topology.

Configure HUB and SPOKE routers to achieve these goals:

1. Configure NHRP authentication using password "Ci$c0123".
2. Configure SPOKE routers to establish direct tunnels between them where LAN routes should be learned from the tunnel interfaces.

**Answer:**

Task 1:

1. Configuration on Hub (R0):

interface Tunnel0
ip address 10.0.0.254 255.255.255.0
no ip split-horizon eigrp 100
ip nhrp network-id 1
ip nhrp authentication Ci$c0123
tunnel source <WAN_Interface>
tunnel mode gre multipoint
tunnel key 100

2. Configuration on Spokes (R1 and R2):

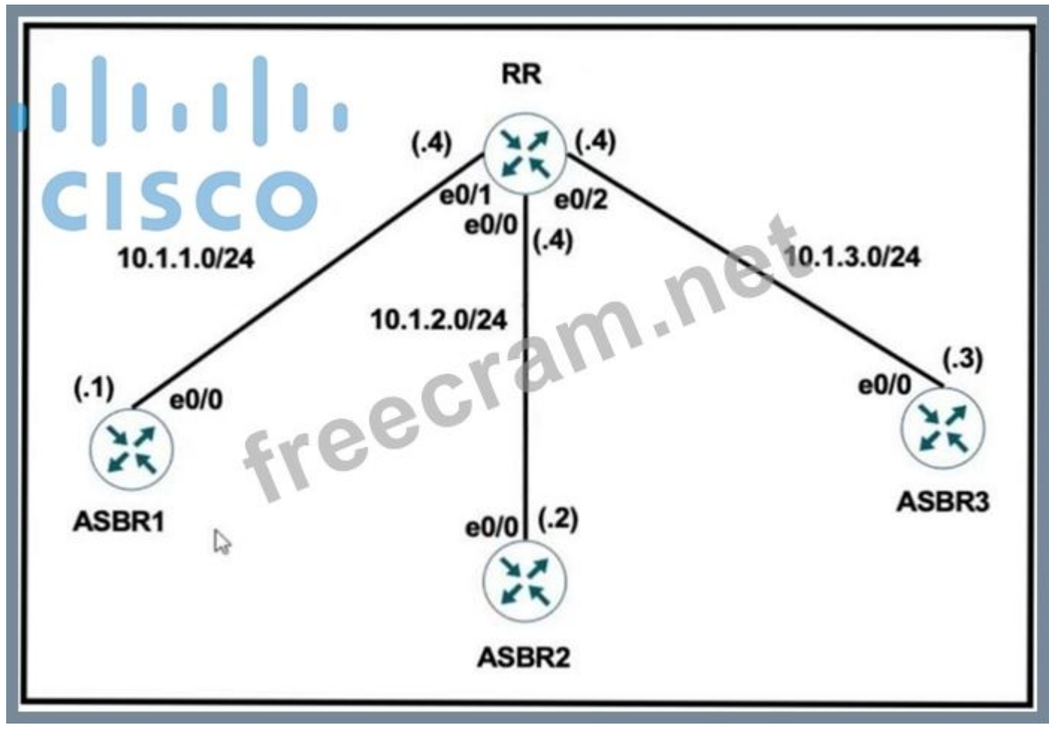
R1:

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp network-id 1

ip nhrp nhs 10.0.0.254
ip nhrp authentication Ci$c0123
ip nhrp map multicast 10.0.0.254
ip nhrp map 10.0.0.254 <Hub_NBMA_IP>
tunnel source <WAN_Interface>
tunnel mode gre multipoint
tunnel key 100
R2:
interface Tunnel0
ip address 10.0.0.2 255.255.255.0
ip nhrp network-id 1
ip nhrp nhs 10.0.0.254
ip nhrp authentication Ci$c0123
ip nhrp map multicast 10.0.0.254
ip nhrp map 10.0.0.254 <Hub_NBMA_IP>
tunnel source <WAN_Interface>
tunnel mode gre multipoint
tunnel key 100
Task 2:
Enable NHRP spoke-to-spoke functionality by adding mapping commands to establish direct tunnels:
R1:
ip nhrp map 10.0.0.2 <R2_NBMA_IP>
ip nhrp shortcut
R2:
ip nhrp map 10.0.0.1 <R1_NBMA_IP>
ip nhrp shortcut
Configure dynamic routing (EIGRP) to learn LAN routes over the tunnel interface:
R0 (Hub):
router eigrp 100
network 10.0.0.0 0.0.0.255
no auto-summary
R1 and R2 (Spokes):
router eigrp 100
network 10.0.0.0 0.0.0.255
network <LAN_Subnet>
no auto-summary
Verification:
1. Verify NHRP Authentication:
show dmvpn
show ip nhrp
2. Verify Spoke-to-Spoke Connectivity:

Ping from PC2 to PC3.
ping 10.100.2.10
3. Verify EIGRP Routes:
show ip route eigrp

**NEW QUESTION: 293**
Refer to the exhibit. 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?




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
**A.** router bgp 100
neighbor IBGP update-source Loopback0
**B.** router bgp 100
neighbor IBGP next-hop-self
**C.** router bgp 100
neighbor 10.1.1.1 next-hop-self

neighbor 10.1.2.2 next-hop-self
neighbor 10.1.3.3 next-hop-self
**D.** router bgp 100
neighbor 10.1.1.1 peer-group IBGP
neighbor 10.1.2.2 peer-group IBGP
neighbor 10.1.3.3 peer-group IBGP
**Answer: (SHOW ANSWER)**
After an MP-EBGP peer relationship is established between ASBRs, an ASBR can advertise the VPNv4 routes of its AS to the other ASBR.

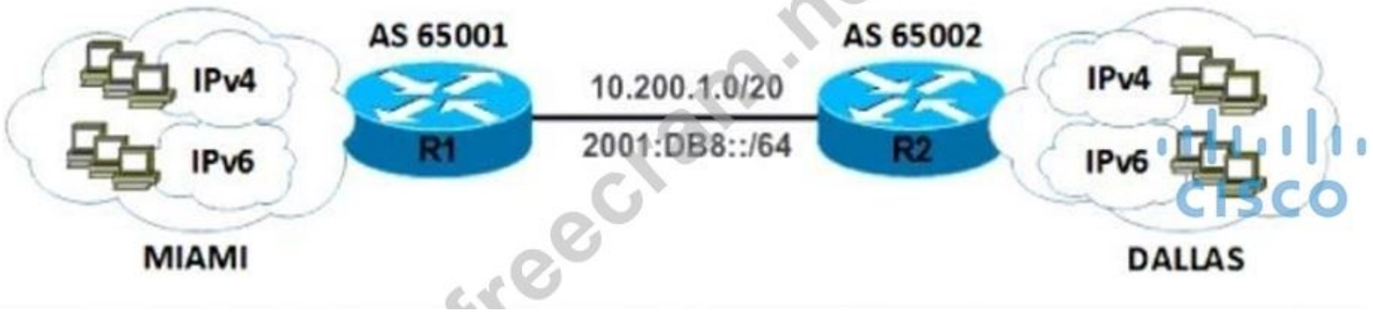
**NEW QUESTION: 294**
What is considered the primary advantage of running BFD?
**A.** reduction in time needed to detect Layer 2 switched neighbor failures
**B.** reduction in CPU needed to detect Layer 2 switch neighbor failures
**C.** reduction in time needed to detect Layer 3 routing neighbor failures
**D.** reduction in CPU needed to detect Layer 3 routing neighbor failures
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 295**
What is a MPLS PHP label operation?
**A.** It improves P router performance by not performing multiple label lookup.
**B.** Downstream node signals to remove the label.
**C.** It uses implicit-NULL for traffic congestion from source to destination forwarding.
**D.** PE removes the outer label before sending to the P router.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 296**
An administrator attempts to download the pack NBAR2 file using TFTP from the CPE router to another device over the Gi0/0 interface.
The CPE is configured as below:
hostname CPE
!
ip access-list extended WAN
<`¦>
remark => All UDP rules below for WAN ID: S421T18E58F90
permit udp any eq domain any
permit udp any any eq tftp
deny udp any any
!
interface GigabitEthernet0/0
<`¦>
ip access-group WAN in
<`¦>

!
tftp-server flash:pp-adv-csr1000v-1612.1a-37-53.0.0.pack
The transfer fails. Which action resolves the issue?
**A.** Change the WAN ACL to permit the UDP port 69 to allow TFTP
**B.** Make the permit udp any eq tftp any entry the last entry in the WAN ACL
**C.** Change the WAN ACL to permit the entire UDP destination port range
**D.** Shorten the file name to the 8+3 naming convention
**Answer: (SHOW ANSWER)**
The TFTP apparently is using the random port for the transfer: TFTP uses UDP as its transport protocol. A transfer request is always initiated targeting port 69, but the data transfer ports are chosen independently by the sender and receiver during the transfer initialization. The ports are chosen at random according to the parameters of the networking stack, typically from the range of ephemeral ports.
https://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol

**NEW QUESTION: 297**
Refer to the exhibit. A network engineer configured routers R1 and R2 with MP-BGP. The engineer noticed that the routers cannot exchange any IPv6 routes; however, the IPv4 neighbor relationship is working fine.

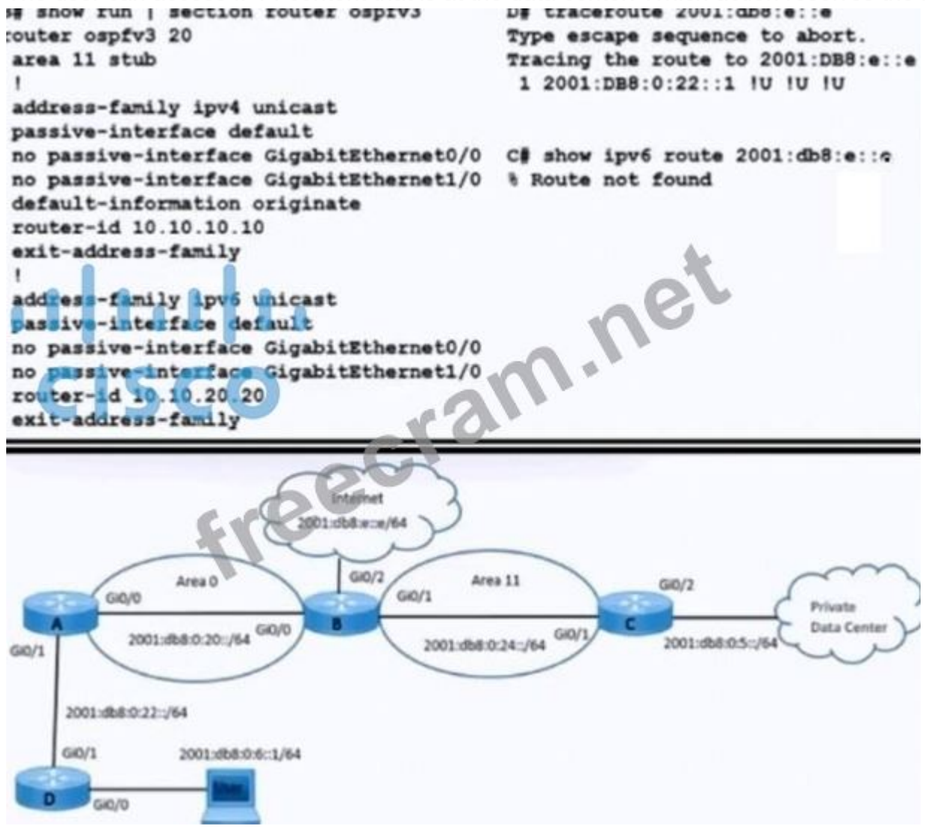



Which configuration must the engineer apply to router R2 to exchange IPv6 routes?
**A.** ipv6 cef
!
interface Loopback100
ipv6 address 2001:DB8:128::2/128
!
interface GigabitEthernet1/0
ipv6 address 2001:DB8:1::2/64
!
router bgp 65002
no bgp default ipv4-unicast
neighbor 2001:DB8:1::1 remote-as 65001
!
address-family ipv6
network 2001:DB8:128::2/128
neighbor 2001:DB8:1::1 activate
**B.** ipv6 unicast-routing
ipv6 cef

!
interface Loopback100
ipv6 address 2001:DB8:128::2/128
!
interface GigabitEthernet1/0
ipv6 address 2001:DB8:1::2/64
!
router bgp 65002
no bgp default ipv4-unicast
neighbor 2001:DB8:1::1 remote-as 65001
!
address-family ipv4
network 2001:DB8:128::2/128
**C.** ipv6 unicast-routing
ipv6 cef
!
interface Loopback100
ipv6 address 2001:DB8:128::2/128
!
interface GigabitEthernet1/0
ipv6 address 2001:DB8:1::2/64
description AS65001 ID B468^AD03G907::1
!
router bgp 65002
no bgp default ipv4-unicast
neighbor 2001:DB8:1::1 remote-as 65001
!
address-family ipv6
network 2001:DB8:128::2/128
neighbor 2001:DB8:1::1 activate
**D.** ipv6 unicast-routing
ipv6 cef
!
interface Loopback100
ipv6 address 2001:DB8:128::2/128
!
interface GigabitEthernet1/0
ipv6 address 2001:DB8:1::2/64
!
router bgp 65002
no bgp default ipv4-unicast

neighbor 2001:DB8:1::1 remote-as 65001
!
address-family ipv6
network 2001:DB8:128::2/128
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 298**
Refer to the exhibit. An enterprise user reports an access issue with IPv6 content on the Internet.
The user can access IPv4 content that is at the data center. Which action resolves the issue with IPv6 content?




**A.** Change Area 11 to Area 0 between routers B and C.
**B.** Enable default information to originate in IPv6 AF on router B.
**C.** Advertise the 2001:db8:e::e/64 route on the router D OSPF process.
**D.** Add a static route for 2001:db8:0:6::1/64 on router B RIB.
**Answer: (SHOW ANSWER)**
The issue lies in the absence of a default route in the IPv6 routing table on router C. Router C needs a default route to forward IPv6 traffic destined for the Internet via router B. In OSPFv3, the default-information originate command is required to propagate a default route to other routers in the OSPF domain.
By enabling default-information originate in the IPv6 address-family configuration on router B, it will advertise the default route to router C, allowing IPv6 traffic to be routed to the Internet.

**NEW QUESTION: 299**
Which protocol supports labeled paths between PE routers in an MPLS network?
**A.** RSVP
**B.** MP-BGP
**C.** IGP
**D.** LDP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 300**
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
```

B.
```
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
```

C.
```
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
```

D.
```
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
```

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: 301**

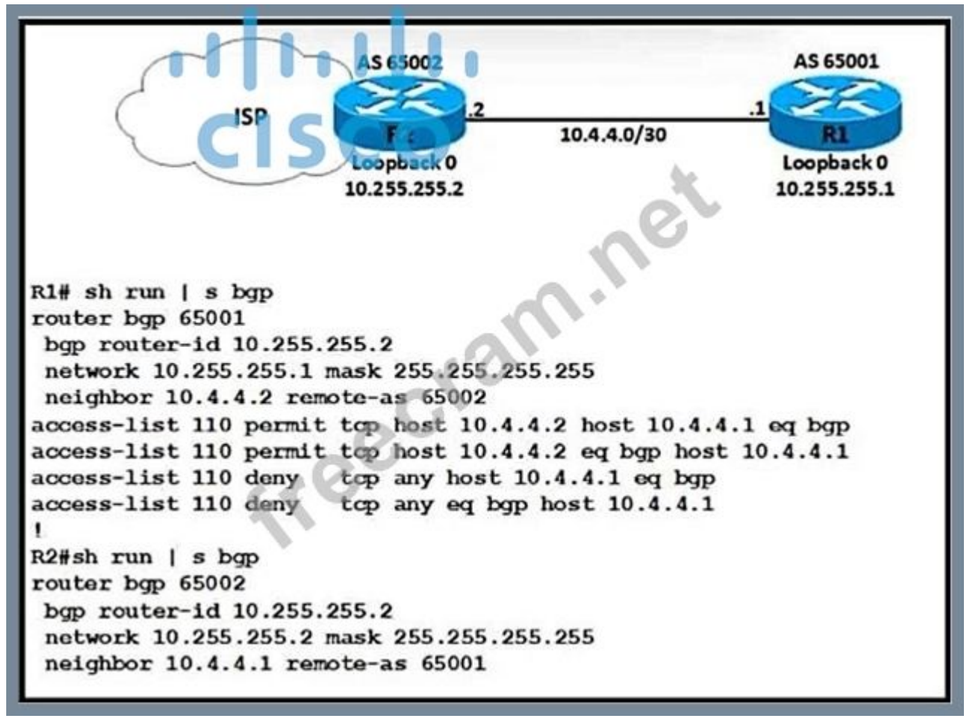
The network administrator is tasked to configure R1 to authenticate telnet connections based on Cisco ISE using RADIUS. ISE has been configured with an IP address of 192.168.1.5 and with a network device pointing towards R1 (192.168.1.1) with a shared secret password of Cisco123. If ISE is down, the administrator should be able to connect using the local database with a username and password combination of admin/cisco123.
The administrator has configured the following on R1:
aaa new-model
!
username admin password cisco123
!
radius server ISE1
address ipv4 192.168.1.5
key Cisco123
!
aaa group server tacacs+ RAD-SERV
server name ISE1
!
aaa authentication login RAD-LOCAL group RAD-SERV
ISE has gone down. The Network Administrator is not able to Telnet to R1 when ISE went down.
Which two configuration changes will fix the issue? (Choose two.)
**A.** aaa authentication login RAD-SERV group RAD-LOCAL local
**B.** line vty 0 4
login authentication RAD-LOCAL
**C.** line vty 0 4
login authentication RAD-SERV
**D.** aaa authentication login RAD-LOCAL group RAD-SERV local
**E.** line vty 0 4
login authentication default
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 302**
The summary route is not shown in the Router_B routing table after this below configuration on Router_A:
interface ethernet 0
description location ID:S4318T3E77F02
ip address 192.168.3.1 255.255.255.0
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
Which Router_A configuration resolves the issue by advertising the summary route to Router_B?
**A.** interface loopback 0

ip address 172.16.96.1 255.255.255.0
interface Ethernet 0
ip address 192.168.3.1 255.255.255.0
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
**B.** interface loopback 0
ip address 172.18.81.1 255.255.255.0
interface Ethernet 0
ip address 192.168.3.1 255.255.255.0
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
**C.** interface loopback 0
ip address 172.16.81.1 255.255.255.0
interface Ethernet 0
ip address 192.168.3.1 255.255.255.0
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
**D.** interface loopback 0
ip address 172.16.79.1 255.255.255.0
interface Ethernet 0
ip address 192.168.3.1 255.255.255.0
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 303**
Refer to the exhibit. A network engineer notices that R1 and R2 cannot establish an eBGP peering.




The following messages appear in the log:

*Dec 21 12:08:59.991: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x6A8B3998:1) NSF delete stale NSF not active
*Dec 21 12:08:59.995: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x44361063:8) NSF no stale paths state is NSF not active
*Dec 21 12:08:59.995: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x6A8B3998:1) Resetting ALL counters.
*Dec 21 12:09:09.819: BG-3-NOTIFICATION: sent to neighbor 10.4.4.2 passive 2/3 (BGP identifier wrong) 4 bytes OAFFFF02
*Dec 21 12:09:09.823: BGP-4-MSGDUMP: unsupported or mal-formatted message received from 10.4.4.2:
*Dec 21 12:09:12.443: 8BGP SESSION-5-ADJCHANGE: neighbor 10.4.4.2 IPv4 Unicast topology base removed from session BGP Notification received
*Dec 21 12:09:00.191: BGP: br global 10.4.4.2 Open active delayed 12288ms (35000ms max, 60% jitter)

Which configuration must the engineer apply to R1 to restore the eBGP peering?

**A.**

```
router bgp 65001
  bgp router-id 10.255.255.2
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit tcp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit tcp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny tcp any host 10.4.4.1 eq 179
access-list 110 deny tcp any eq 179 host 10.4.4.1
```

```
router bgp 65001
  bgp router-id 10.255.255.2
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit udp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit udp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny udp any host 10.4.4.1 eq 179
access-list 110 deny udp any eq 179 host 10.4.4.1
```

B.

```
router bgp 65001
  bgp router-id 10.255.255.1
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit udp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit udp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny udp any host 10.4.4.1 eq 179
access-list 110 deny udp any eq 179 host 10.4.4.1
```

C.

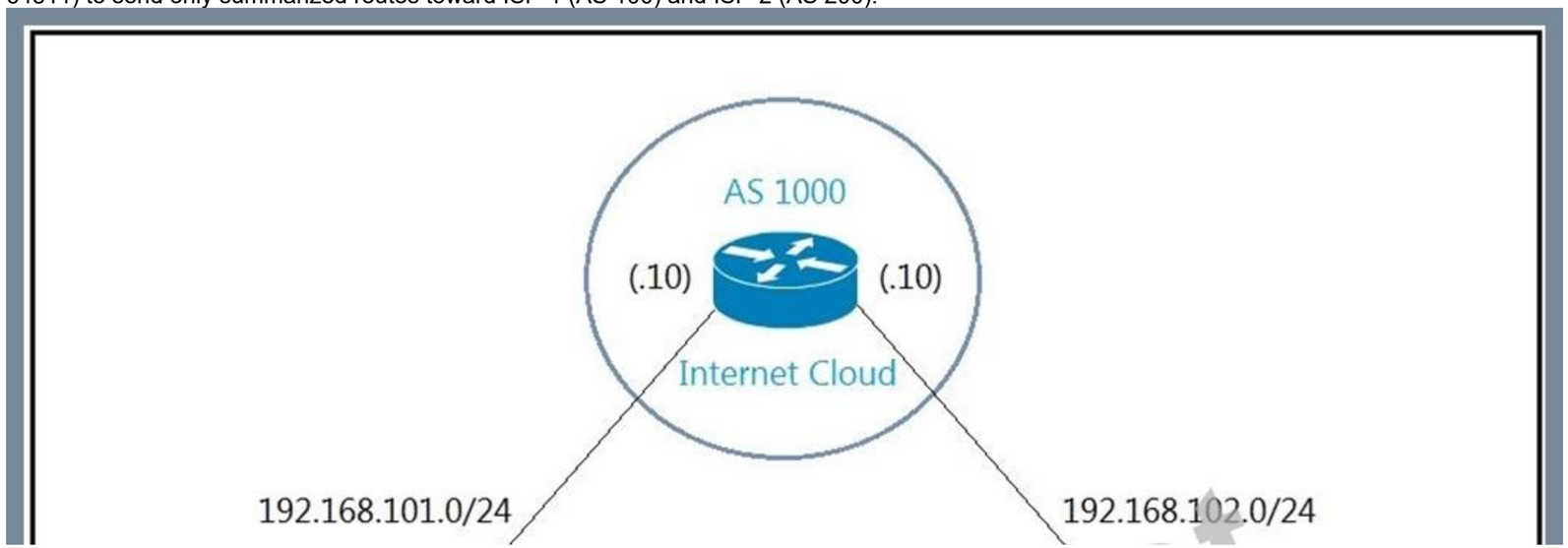
```
router bgp 65001
  bgp router-id 10.255.255.1
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit tcp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit tcp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny   tcp any host 10.4.4.1 eq 179
access-list 110 deny   tcp any eq 179 host 10.4.4.1
```

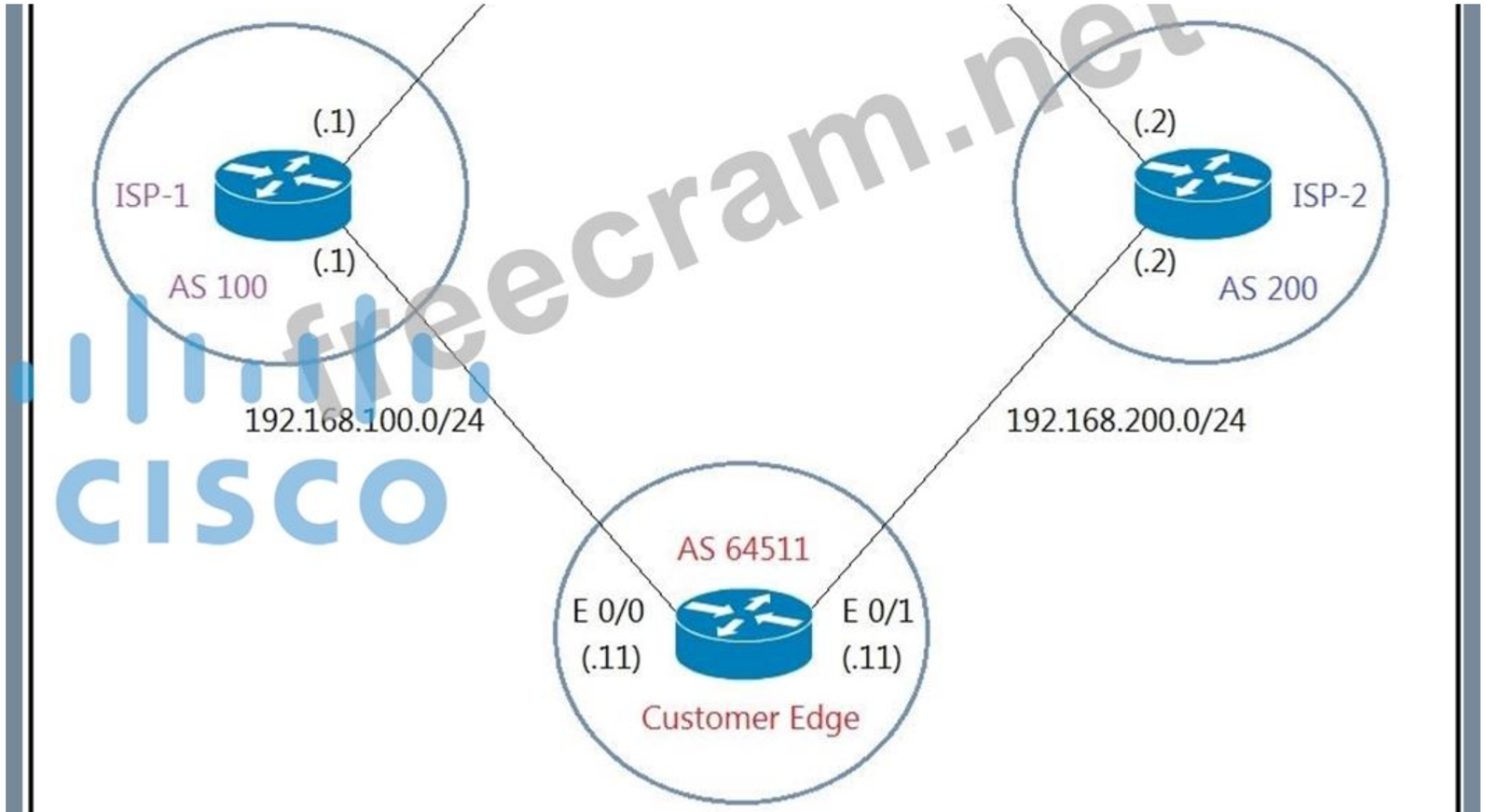
D.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 304**

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






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

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

**A.**

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

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

C.
```
interface E 0/0
 ip bgp suppress-map BLOCK_SPECIFIC
!
interface E 0/1
 ip bgp suppress-map BLOCK_SPECIFIC
!
 ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22 ge 24
!
route-map BLOCK_SPECIFIC permit 10
 match ip address prefix-list PL_BLOCK_SPECIFIC
```

D.
```
ip prefix-list PL_BLOCK_SPECIFIC deny 172.16.20.0/22 ge 22
ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22
!
route-map BLOCK_SPECIFIC permit 10
 match ip address prefix-list PL_BLOCK_SPECIFIC
!
router bgp 64511
 aggregate-address 172.16.20.0 255.255.252.0 suppress-map BLOCK_SPECIFIC
```

**Answer: (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.

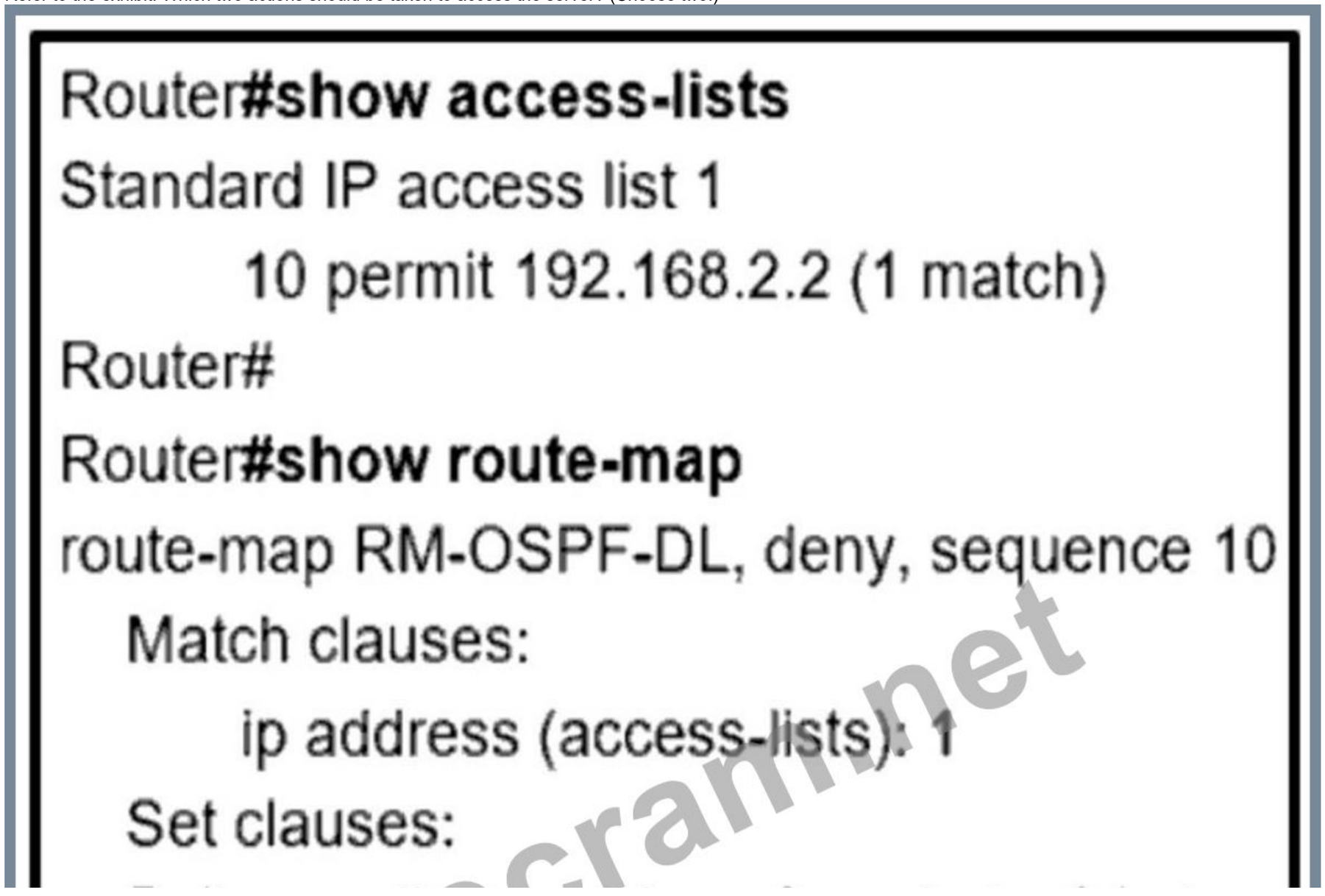
**NEW QUESTION: 305**

An engineer creates a Cisco DNA Center cluster with three nodes, but all the services are running on one host node.

Which action resolves this issue?

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

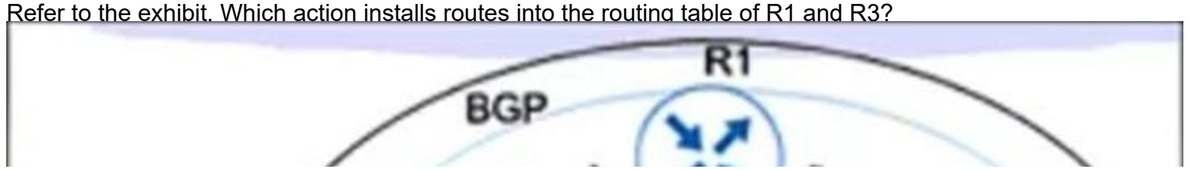
**NEW QUESTION: 306**
Refer to the exhibit. Which two actions should be taken to access the server? (Choose two.)

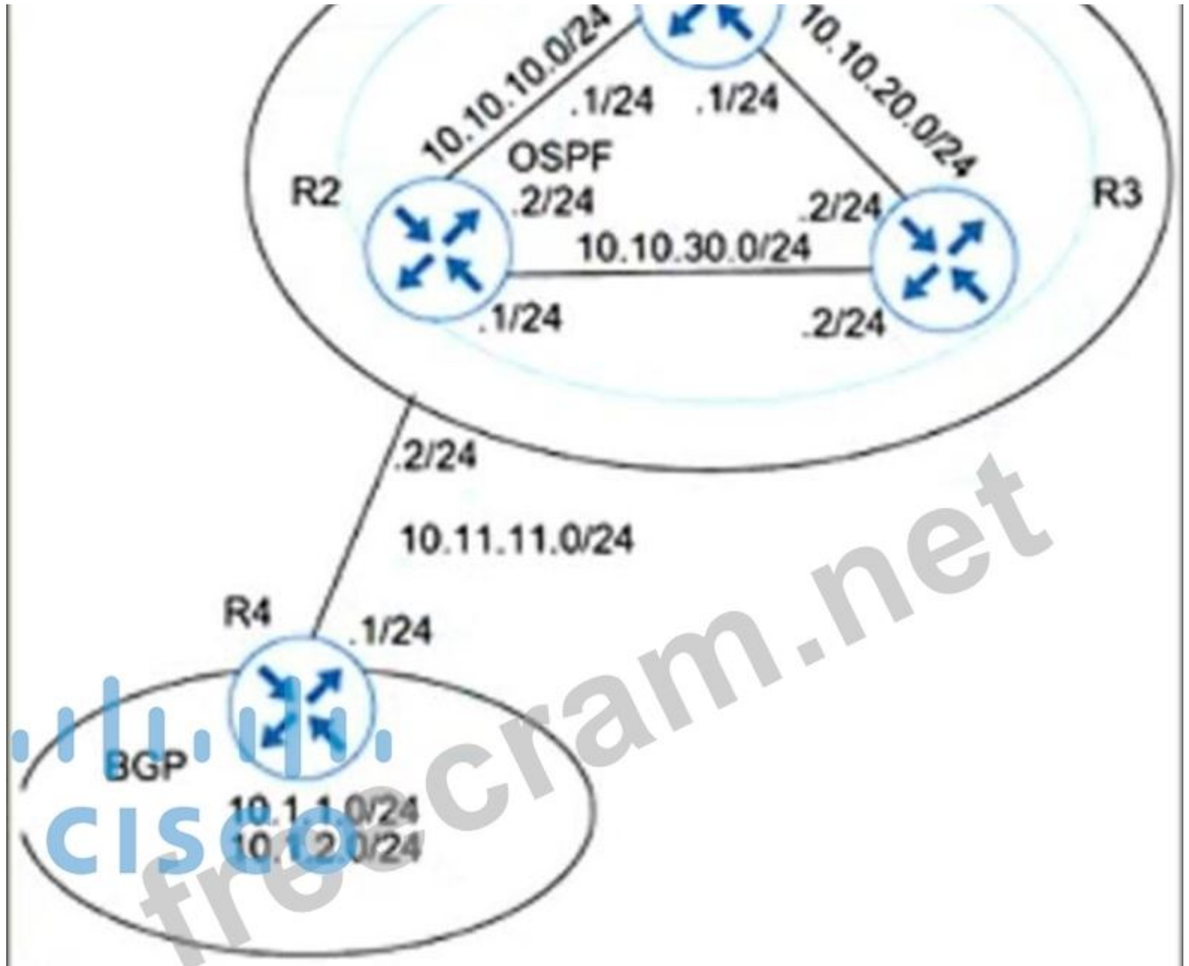


```
    Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
    network 192.168.1.1 0.0.0.0 area o
    network 192.168.12.0 0.0.0.255 area 0
    distribute-list route-map RM-OSPF-DL in
Router#
```

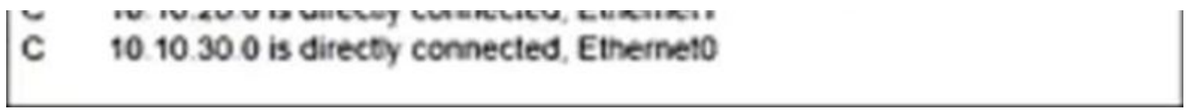
**A.** Modify the access list to add a second line of permit ip any.
**B.** Modify distribute list seq 10 to permit the route to 192.168.2.2.
**C.** Add a sequence 20 in the route map to permit access list 1.
**D.** Modify the access list to deny the route to 192.168.2.2.
**E.** Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 307**
Refer to the exhibit. Which action installs routes into the routing table of R1 and R3?





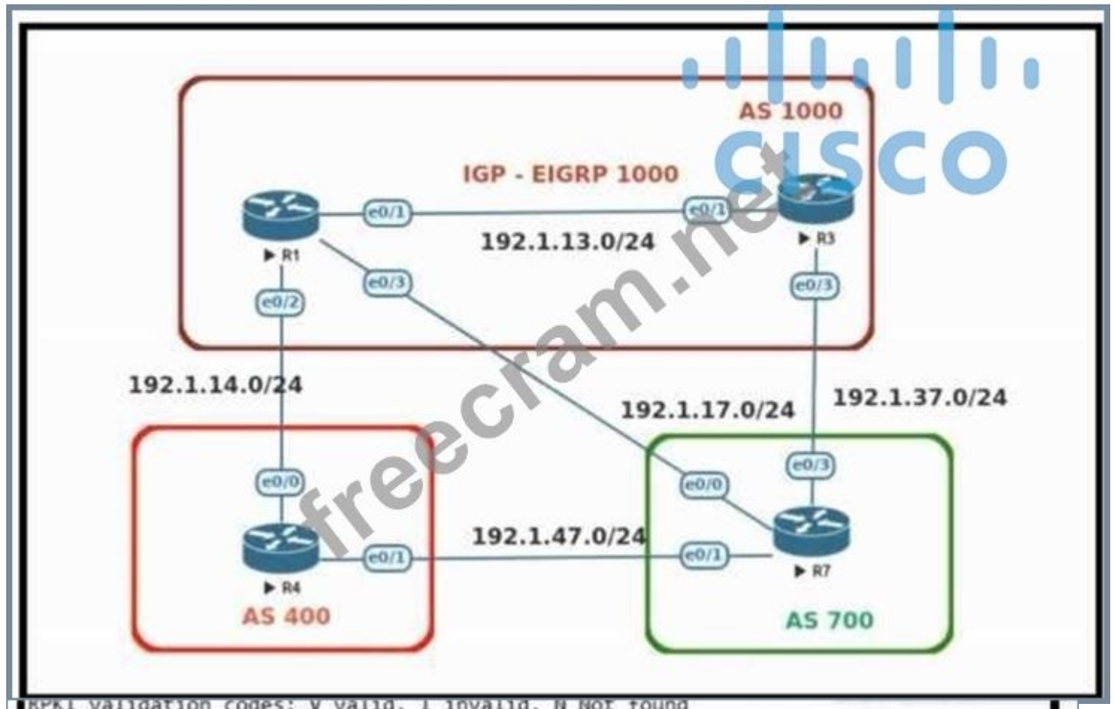

```
R3# show ip bgp BGP
table version is 4, local router ID is 10.10.20.2 Status
codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network          Next Hop        Metric LocPrf Weight Path
*i10.1.1.0        10.11.11.1           0    100      0        400 i
*i10.1.2.0        10.11.11.1           0    100      0        400 i

R3# show ip route
O       10.10.10.0 [110/75] via 10.10.30.1, 01:50:45, Ethernet0
O       10.10.10.0 [110/75] via 10.10.20.1, 01:50:45, Ethernet1
C       10.10.20.0 is directly connected, Ethernet1
```




**A.** BGP Synchronization has been enabled. Disable synchronization.
**B.** BGP weight is set to 0. Configure a higher weight for these routes.
**C.** IGP does not have a route to R4. Rectify route reachability.
**D.** BGP has not been redistributed into the IGP. Redistribute BGP.
**Answer: (SHOW ANSWER)**
In the output of show ip bgp, R3 learns the BGP routes 10.1.1.0/24and 10.1.2.0/24 with next hop 10.11.11.1, which is the IP of R4. However, these routes are not present in R3's routing table. For BGP to install a route into the routing table, the next-hop IP address must be reachable via the IGP.
Since there is no IGP route to 10.11.11.1 on R3, the BGP routes are considered invalid and are not installed into the routing table. Fixing the reachability to R4 (e.g., by advertising 10.11.11.0/24into OSPF or another IGP) will resolve the issue.

**NEW QUESTION: 308**
Select three benefits of setting up a MPLS Network from the below options. (Choose three.)
**A.** Connection less Service
**B.** Security as good as connection-oriented VPNs
**C.** Integrated QoS support
**D.** All variations of Static routes are supported
**E.** Provides IPS level intelligence to filter packets.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 309**
Refer to the exhibit. R1 should have BGP routes marked with an "i" (IGP origin code). Which configuration resolves the issue?




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 ? |



**A.** R1
route-map RC permit
match ip address 1
set origin igp

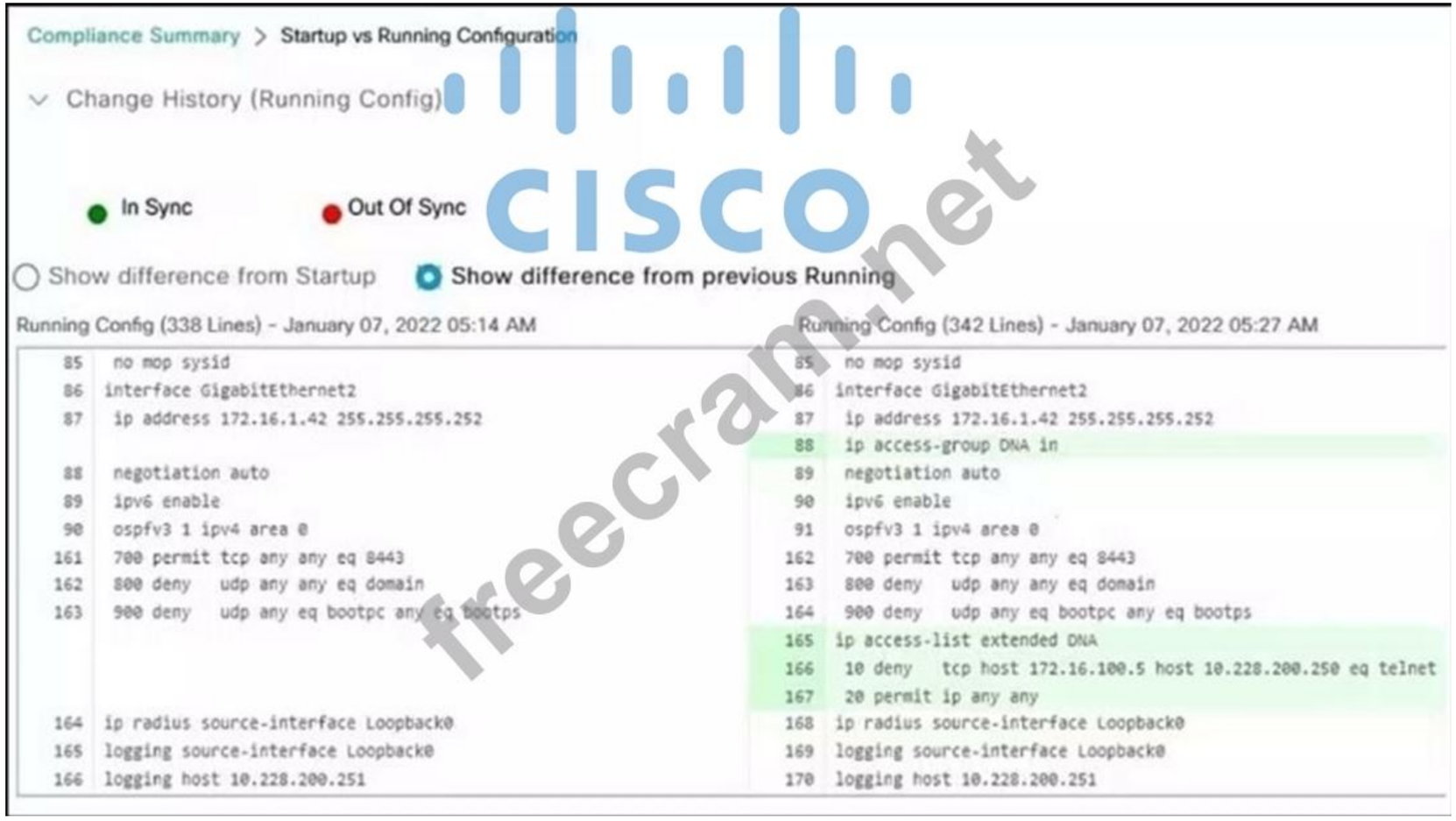
**B.** R7
route-map RC permit 10
match ip address 1
set metric 1

**C.** R7
route-map RC permit 10

match ip address 1
set origin igp
**D.** R1
route-map RC permit 10
match ip address 1
set metric 1
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 310**
Which configuration enables the VRF that is labeled "Inet" on FastEthernet0/0?
**A.** R1(config)# ip vrf Inet
R1(config-vrf)#ip vrf FastEthernet0/0
**B.** R1 (conflg)#ip vrf Inet FastEthernet0/0
**C.** R1(config)# ip vrf Inet
R1(config-vrf)#interface FastEthernet0/0
R1(config-if)#ip vrf forwarding Inet
**D.** R1 (config)#router ospf 1 vrf Inet
R1 (config-router)#ip vrf forwarding FastEthernet0/0
**Answer: C (LEAVE A REPLY)**
The first command "R1(config)# ip vrf Inet" creates vrf Inet while the two last commands associate the VRF with interface Fa0/0.

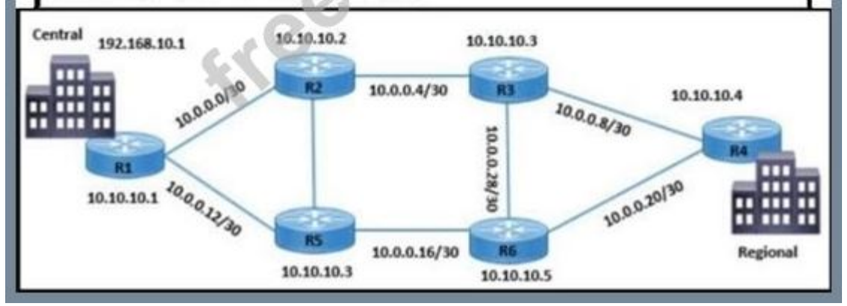
**NEW QUESTION: 311**
Refer to the exhibit. After an engineer updates the configuration on the device, they noticed unexpected behavior. Which command resolves the issue by completely replacing the startup configuration?




**A.** configure replace nvram:startup-config
**B.** copy system:running.config nvram:startup-config
**C.** configure replace nvram:private-config
**D.** copy running-config startup-config
**Answer: (SHOW ANSWER)**
configure replace nvram:startup-config replaces the current running configuration with the saved startup configuration, removing unintended changes and restoring the device to the exact startup- config state. This is the correct command when a full replacement is required rather than merging configuration lines.

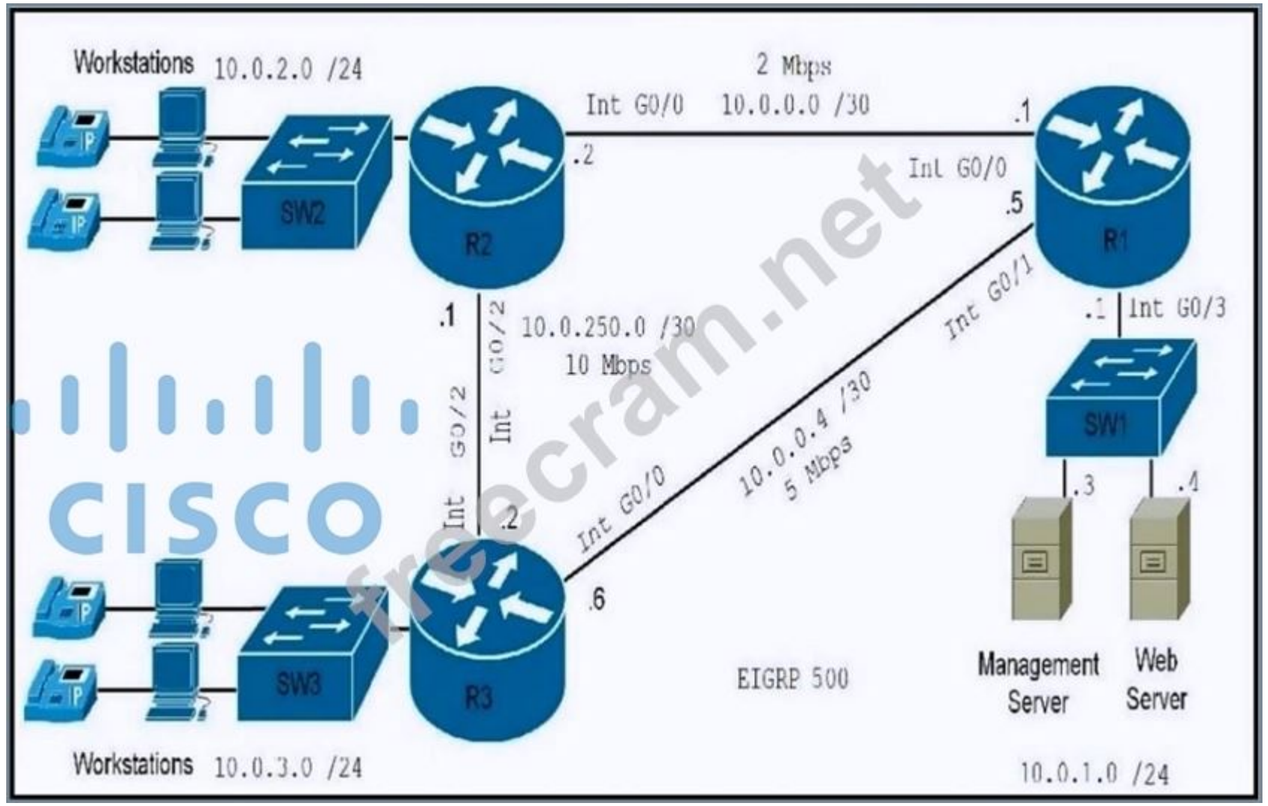
**NEW QUESTION: 312**
Refer to the exhibit. Traffic from R3 to the central site does not use alternate paths when R3 cannot reach 10.10.10.2. Traffic on R3 destined to R4 takes an alternate route via 10.10.10.6 when 10.10.10.4 is not accessible from R3. Which configuration switches traffic destined to

```
R3#show ip sla statistics
IPSLAs Latest Operation Statistics
IPSLA operation id: 10
Type of operation: icmp-echo
        Latest RTT: 24 milliseconds
Latest operation start time: *21:26:43.211 UTC Sat Sep 18 2021
Latest operation return code: OK
Number of successes: 75
Number of failures: 0
Operation time to live: Forever

IPSLA operation id: 20
Type of operation: icmp-echo
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: *21:26:47.499 UTC Sat Sep 18 2021
Latest operation return code: No connection
Number of successes: 128
Number of failures: 459
Operation time to live: Forever
```




**A.** R3(config)#ip route 192.168.10.1 255.255.255.255 10.10.10.2 track 20
**B.** R3(config)#track 20 ip sla 20 reachability
**C.** R2(config)#ip route 10.10.10.3 255.255.255.255 10.0.0.6
**D.** R6(config)#ip route 10.10.10.3 255.255.255.255 10.0.0.30
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 313**
Refer to the exhibit. An engineer must route the management server traffic to the network 10.0.250.0 over the 2 Mbps link. Which configuration accomplishes this task on R1?






**A.** route-map advrt permit 10
match ip address 110
set ip next-hop 10.0.02
!
access-list 110 permit ip host 10.0.1.3 10.0.250.0 0.0.0.3
!
interface GigabitEthernet0/3
ip policy route-map advrt
**B.** interface GigabitEthernet0/1
bandwidth 20000
**C.** route-map advrt permit 10
match ip address 110
set ip next-hop 10.0.0.1
!
access-list 110 permit ip host 10.0.1.3 10.0.250.0 0.0.0.3
!
interface GigabitEthernet0/3
ip policy route-map advrt
**D.** interface GigabitEthernet0/0

bandwidth 20000

**Answer: (SHOW ANSWER)**

The requirement is to route traffic from the management server (10.0.1.3) to the 10.0.250.0/30 network over the 2 Mbps link. Policy-Based Routing (PBR) is used to accomplish this task by overriding the default routing behavior.

The access list 110 matches the traffic sourced from the management server destined for the
10.0.250.0/30 network. The route map advrt matches traffic using the access list and sets the next hop to 10.0.0.2 (the IP address on R2's interface connected to R1 via the 2 Mbps link). The route map is applied as a policy on GigabitEthernet0/3, which is the interface connected to the management server. This ensures that traffic from the management server is routed over the specified link.

**NEW QUESTION: 314**

Refer to the exhibit. A network administrator successfully logs in to a switch using SSH from a RADIUS server. When the network administrator uses a console port to access the switch, the RADIUS server returns shell:priv-lvl=15" and the switch asks to enter the enable command.

When the command is entered, it gets rejected.

Which command set is used to troubleshoot and resolve this issue?

```
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.** line con 0
aaa authorization console
authorization exec
!
line vty 0 4

transport input ssh
**B.** line con 0
aaa authorization console
!
line vty 0 4
authorization exec
**C.** line con 0
aaa authorization console priv15
!
line vty 0 4
authorization exec
**D.** line con 0
aaa authorization console
authorization priv15
!
line vty 0 4
transport input ssh
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 315**
Refer to the exhibit. Which set of commands restore reachability to loopback0?

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



**A.** interface loopback0

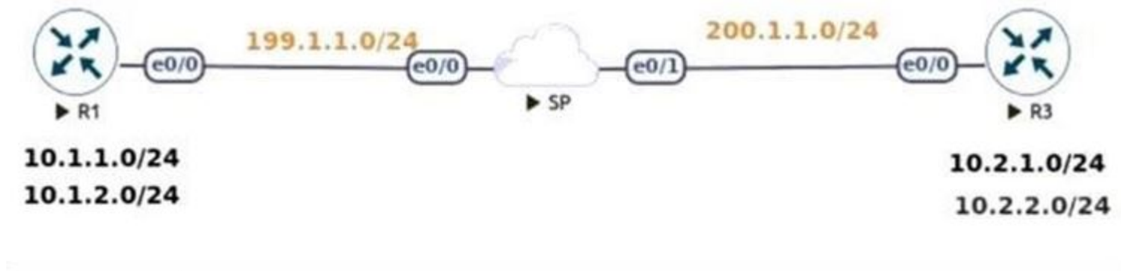
ip address 4.4.4.4 255.255.255.0
ip ospf interface area 10
**B.** interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network broadcast
**C.** interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf interface type network
**D.** interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network point-to-point
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 316**
What are the two goals of micro BFD sessions? (Choose two.)
**A.** Run the BFD session with 3x3 ms hello timer.
**B.** Each member link of a link aggregation group must run BFD.
**C.** Continuity for each member link of a link aggregation group must be verified.
**D.** Any member link on a link aggregation group must run BFD.
**E.** The high bandwidth member link of a link aggregation group must run BFD.
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 317**
Which group of components works together to create an MPLS VPN?
**A.** route target, label distribution protocol, and QoS
**B.** route target, MP-BGP peering, and MPLS forwarding
**C.** MPLS forwarding, OSPF routing protocol, and BGP peering
**D.** route target, OSPF routing protocol, and label distribution protocol
**Answer: (SHOW ANSWER)**
An MPLS VPN is built by using MP-BGP to carry VPN routes, route targets to control VPN route import and export between VRFs, and MPLS forwarding to transport labeled traffic across the provider core. These components together provide reachability and separation between customer VPNs.

**NEW QUESTION: 318**
Refer to the exhibit. An engineer must establish a point-to-point GRE VPN between R1 and the remote site. Which configuration accomplishes the task for the remote site?



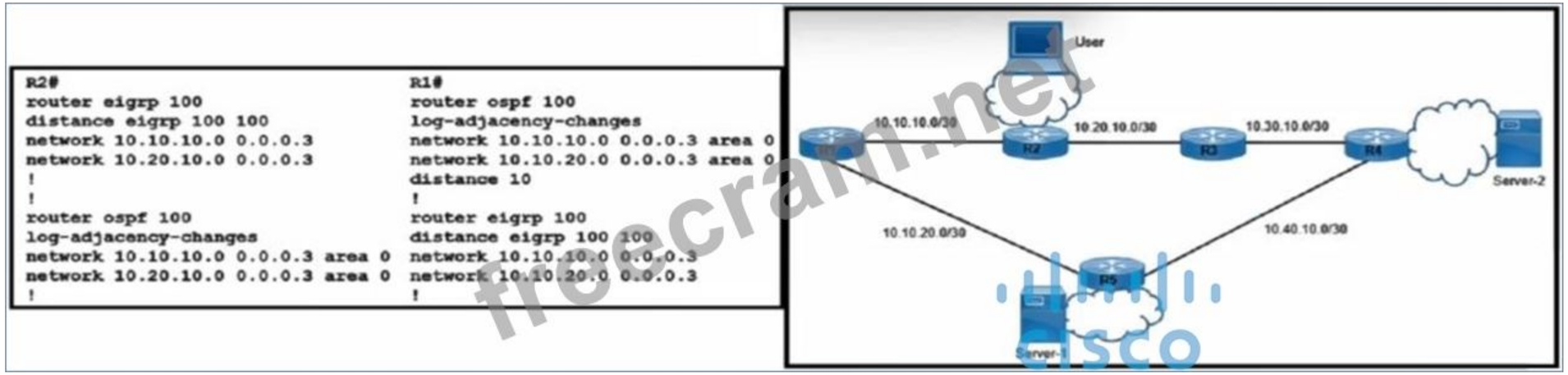

```
R1#sh interfaces tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.1.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 199.1.1.1, destination 200.1.1.3
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
```



**A.** Interface Tunnel1
tunnel source 199.1.1.1
tunnel destination 200.1.1.3
ip address 192.168.1.3 255.255.255.0
**B.** Interface Tunnel1
tunnel source 200.1.1.3
tunnel destination 199.1.1.1
ip address 192.168.1.1.255.255.255.0
**C.** Interface Tunnel1
tunnel source 200.1.1.3

tunnel destination 199.1.1.1
ip address 192.168.1.3.255.255.255.0
**D.** Interface Tunnel
lunnel source 199.1.1.1
tunnel destination 200.1.1.3
ip address 192.168.1.1.255.255.255.0
**Answer: C (LEAVE A REPLY)**
Based on the exhibit, the GRE tunnel configuration on R1 uses the following parameters:
Tunnel source: 199.1.1.1
Tunnel destination: 200.1.1.3
To establish the point-to-point GRE VPN for the remote site (R3), the configuration must mirror these settings, but with the source and destination reversed. Therefore, the correct configuration should use:
Tunnel source: 200.1.1.3
Tunnel destination: 199.1.1.1

**NEW QUESTION: 319**
Refer to the exhibit. The user experiences random packet drops when accessing Server-1 but does not have any issues when reaching out to Server-2. Which action resolves the issue?




**A.** Remove the distance 10 under the OSPF process on R1.
**B.** Modify the distance 10 under the OSPF process on R1 to 90.
**C.** Configure the distance under the EIGRP process to 10 on R1.
**D.** Configure the distance under the EIGRP process to 10 on R2.
**Answer: (SHOW ANSWER)**
In the provided configuration, R1 has a modified OSPF administrative distance set to 10. By default, OSPF has an administrative distance of 110, and EIGRP has an administrative distance of 90. Lowering OSPF's distance to 10 makes OSPF routes preferred over EIGRP routes, potentially causing suboptimal routing and packet drops when accessing Server-1.
By removing the distance 10under the OSPF process on R1, the default OSPF administrative distance of 110 is restored, and EIGRP routes (AD 90) will take precedence as intended, resolving the routing issue.

**NEW QUESTION: 320**
Refer to the exhibit. A network engineer cannot remote access R3 using Telnet from switch S1.
Which action resolves the issue?


**A.** Add the login admin command on the switch.
**B.** Add the transport input telnet command on R3.
**C.** Allow the inbound connection via the exec command on R3.
**D.** Allow to use the ssh -| admin 10.0.0.1 command on the switch.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 321**
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: D (LEAVE A REPLY)**
The configuration uses SNMPv3 with authentication and DES encryption, which means the security level must be authPriv. The UNKNOWNUSERNAME and WRONGDIGEST errors indicate the SNMPv3 user credentials

do not match, especially the authentication details, and successful encrypted communication also requires the correct privacy settings. Configuring the correct authentication and privacy passwords under authPriv resolves the issue.

**NEW QUESTION: 322**
Refer to the exhibit. An engineer configured two ASBRs, 10.4.17.6 and 10.4.15.5, in an OSPF network to redistribute identical routes from BGR. However, only prefixes from 10.4.17.6 are installed into the routing table on R1. Which action must the engineer take to achieve load sharing for the BGP-originated prefixes?

```
R1#show ip route ospf

     10.0.0.0/24 is subnetted, 7 subnets

O E1    10.4.9.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0

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

O E1    10.4.49.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0

O E1    10.4.59.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0
```

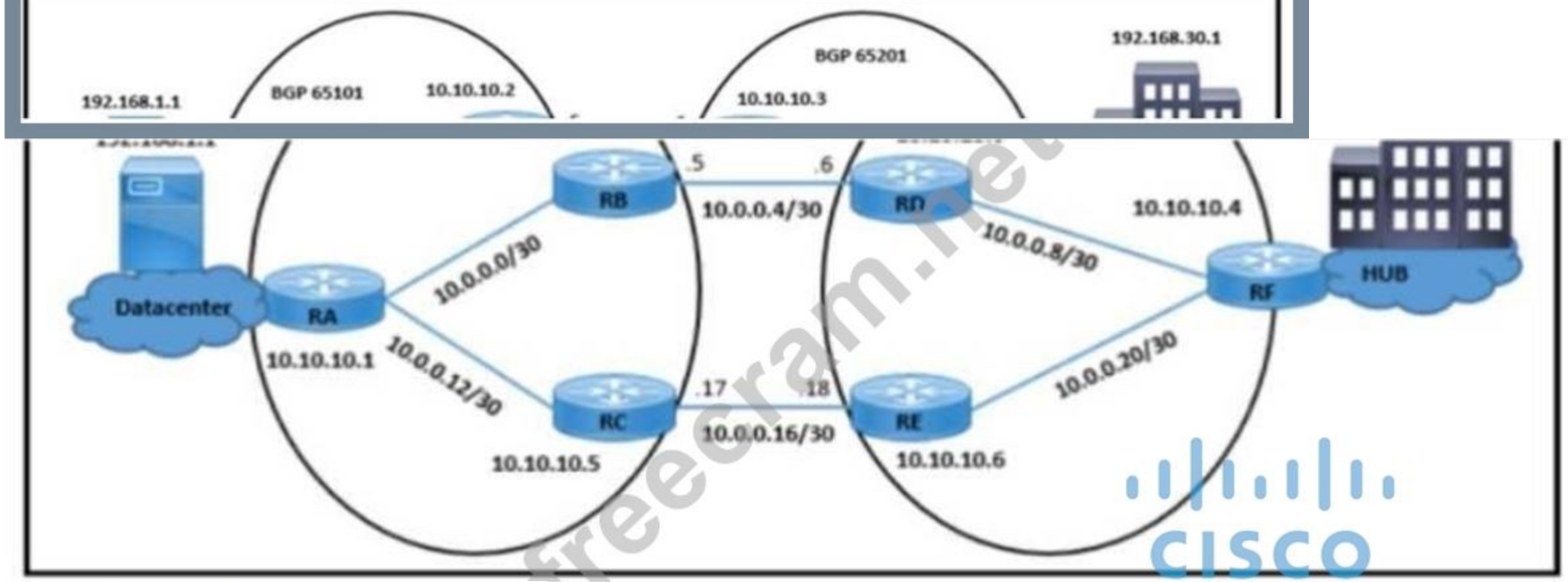


**A.** The ASBRs are advertising the redistributed prefixes as Type 1 and must be modified to Type 2
**B.** The ASBRs are advertising the redistributed prefixes with the iBGP metric and must be modified to Type 1 on ASBR 10.4.17.6.
**C.** The admin distance of the prefixes must be adjusted to 20 on ASBR 10.4.15.5 to advertise prefixes to R1 identically from both ASBRs.
**D.** The ASBRs are advertising the redistributed prefixes with a different admin distance and must be changed to 110 on ASBR 10.4.15.5.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 323**
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 Prefix Guard
**B.** IPv6 Snooping
**C.** IPv6 Destination Guard
**D.** IPv6 Router Advertisement Guard
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 324**
Refer to the exhibit. A customer finds that traffic from the application server (192.168.1.1) to the HUB site passes through a congested path that causes random packet drops. The NOC team influences the BGP path with MED on RB. But RD still sees that traffic coming from RA is not taking an alternate route. Which configuration resolves the issue?

```
RD#show  ip bgp 192.168.1.1
Advertised to update-groups:
        3
  65101
    10.10.10.2 (metric 2) from 10.10.10.2 (10.10.10.2)
      Origin IGP, metric 100, localpref 100, weight 65535, valid, external,
best
  65101
    10.0.0.17 (metric 2) from 10.10.10.6 (172.16.20.1)
      Origin IGP, metric 0, localpref 100, valid, internal

RB#show  ip bgp 192.168.1.1
BGP routing table entry for 192.168.1.1/32, version 10
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
        2
  Local
    10.10.10.1 (metric 2) from 10.10.10.1 (192.168.1.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best
```




RD(config)#**router bgp 65201**
RD(config-router)#**no neighbor 10.10.10.2 weight 65535**

**A.**

```
RB(config)#router bgp 65101
RB(config-router)#no neighbor 10.10.10.3 route-map HIGH-LP out
```

**B.**

```
RC(config)#router bgp 65101
RC(config-router)#neighbor 10.10.10.6 route-map HIGH-LP out
```

**C.**

```
RB(config)#router bgp 65101
RB(config-router)#neighbor 10.10.10.3 weight 50
```

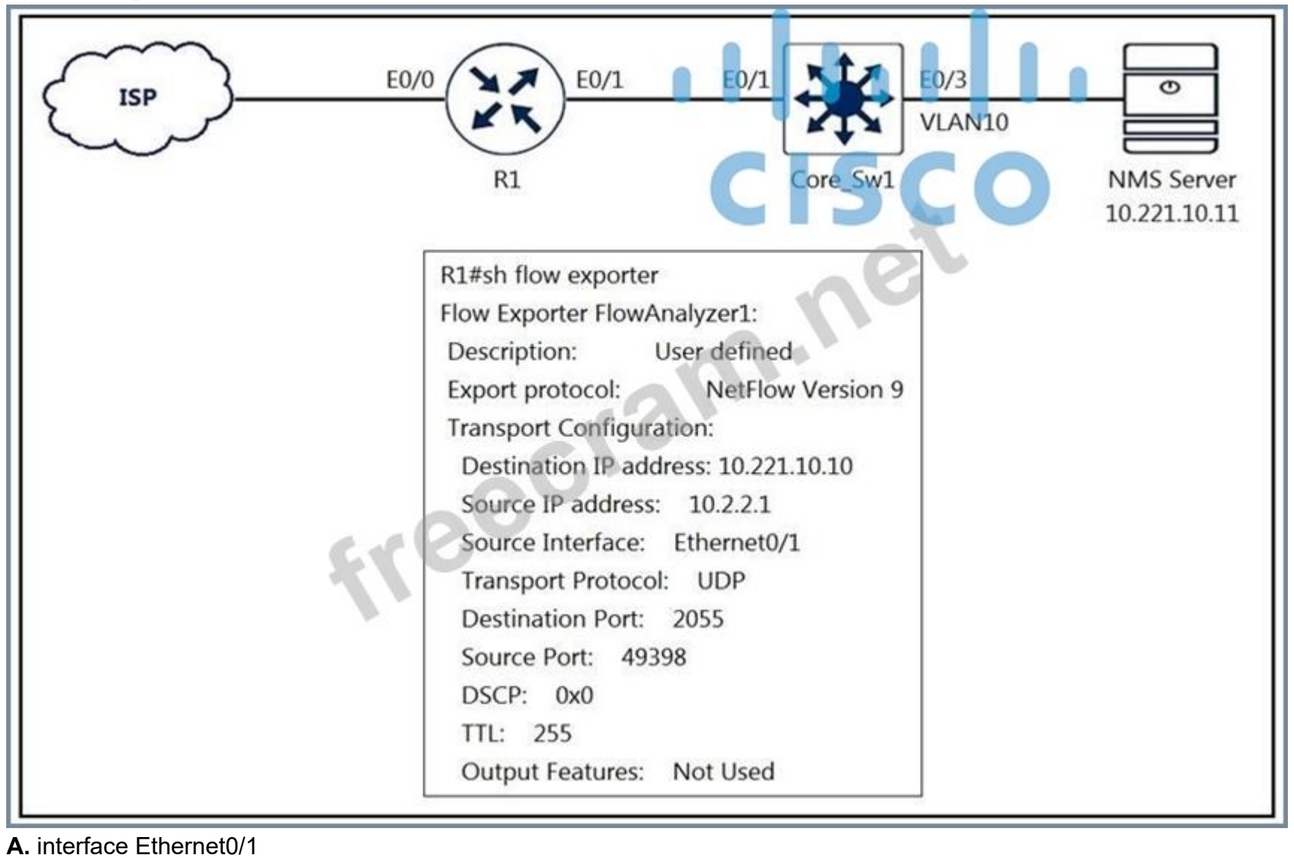
**D.**

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 325**

Refer to the exhibit. An engineer configured NetFlow on R1, but the NMS server cannot see the flow from R1.

Which configuration resolves the issue?



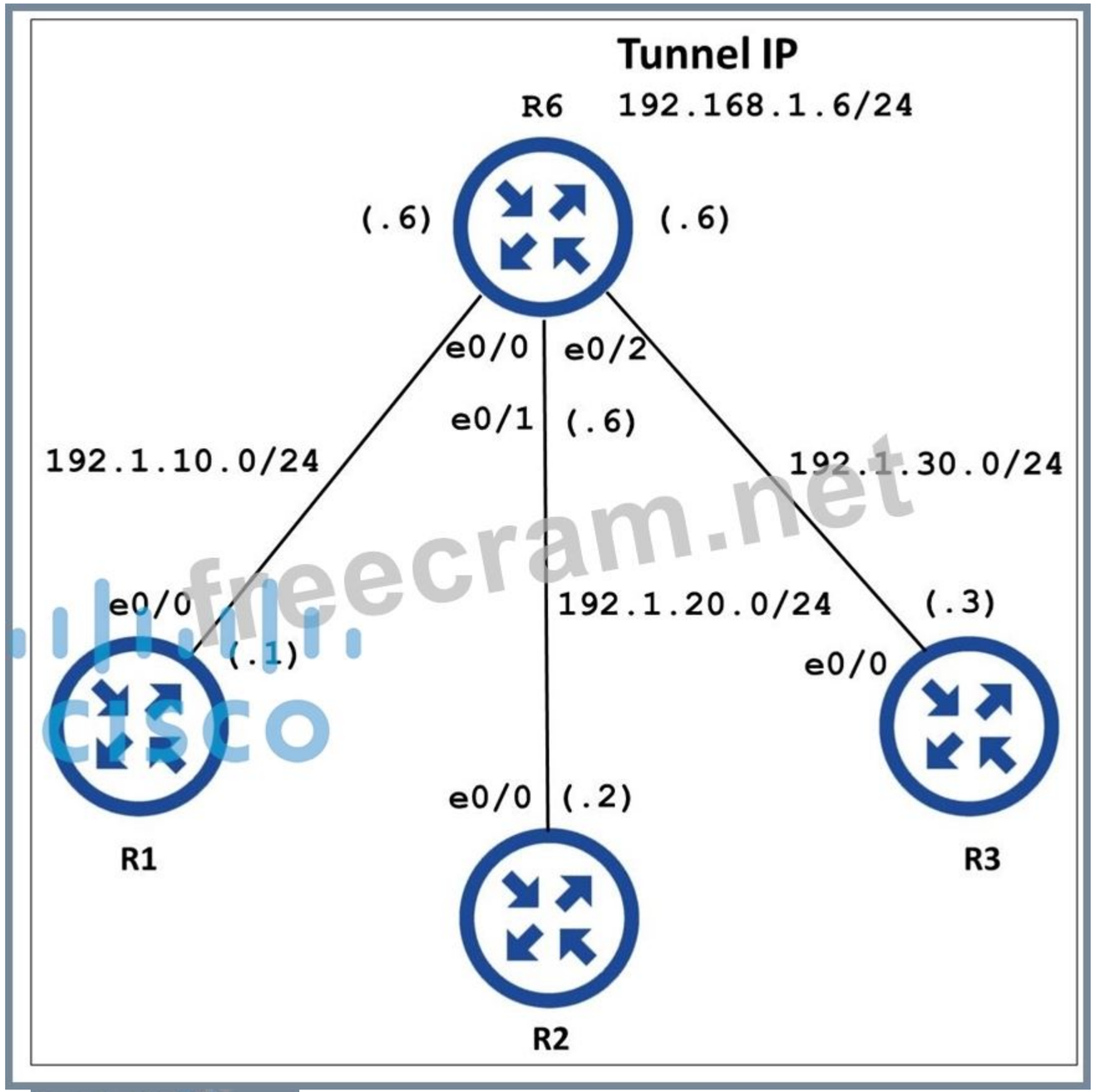

**A.** interface Ethernet0/1
flow-destination 10.221.10.11

**B.** flow monitor Flowmonitor1
destination 10.221.10.11

**C.** interface Ethernet0/0

flow-destination 10.221.10.11
**D.** flow exporter FlowAnalyzer1
destination 10.221.10.11
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 326**
Refer to the exhibit. An engineer must establish multipoint GRE tunnels between hub router R6 and branch routers R1, R2, and R3. Which configuration accomplishes this task on R1?




A.

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.6
```

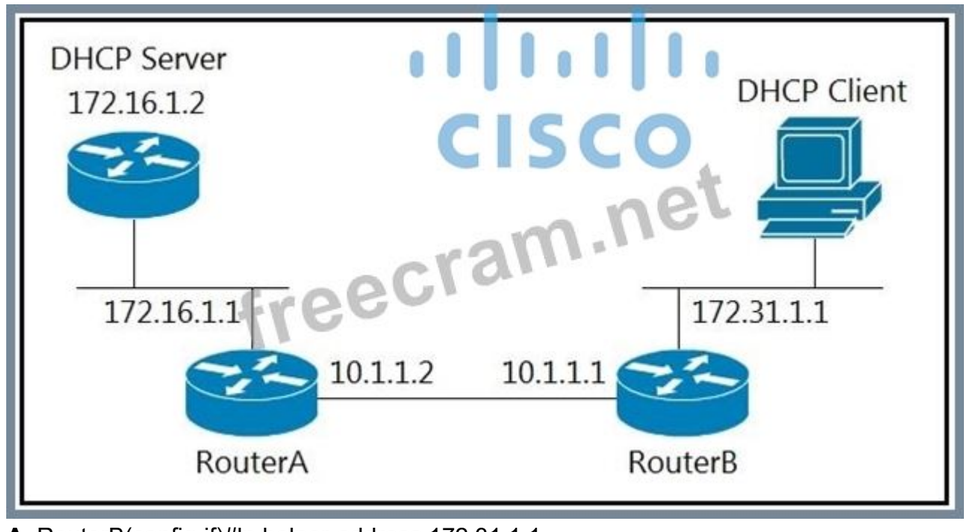
B.
```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.6
```
C.
```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/0
 tunnel mode gre multipoint
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.1
 ip nhrp map 192.168.1.2 192.1.20.2
 ip nhrp map 192.168.1.3 192.1.30.3
```
D.
```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.1
 ip nhrp map 192.168.1.2 192.1.20.2
 ip nhrp map 192.168.1.3 192.1.30.3
```
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 327**

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

```
Interface fastethernet 0/0
 description Client DHCP
  ip address 172.31.1.1 255.255.255.0
 !
 ip route 172.16.1.0 255.255.255.0 10.1.1.2
```

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





**A.** RouterB(config-if)#Ip helper-address 172.31.1.1
**B.** RouterB(config-if)#Ip helper-address 255.255 255.255
**C.** RouterB(config-if)#Ip helper-address 172.16.1.1
**D.** RouterB(config-if)#Ip helper-address 172.16.1.2
**Answer: (SHOW ANSWER)**
The DHCP client broadcasts on the 172.31.1.0/24 subnet, and RouterB must relay those broadcasts to the remote DHCP server. The ip helper-address on RouterB's FastEthernet0/0 interface must point to the actual DHCP server address, which is 172.16.1.2.

**NEW QUESTION: 328**
While troubleshooting connectivity issues to a router, these details are noticed:
- Standard pings to all router interfaces, including loopbacks, are
successful.
- Data traffic is unaffected.
- SNMP connectivity is intermittent.
- SSH is either or disconnects frequently.
Which command must be configured first to troubleshoot this issue?
**A.** Show policy-map control-plane
**B.** Show policy-map
**C.** Show interface inc drop
**D.** Show ip route
**Answer: (SHOW ANSWER)**
The "show policy-map control-plane" is used to display the service-policy associated to the control-plane. It also shows the packets that matched the class-map. An example of the output of this command is shown below:

```
Control Plane

 Service-policy input: CoPP_policy

   Class-map: Telnet_class (match-all)
     62 packets, 2866 bytes
     5 minute offered rate 0 bps, drop rate 0 bp
     Match: access-group name CoPP_traffic
     police:
         cir 8000 bps, bc 1500 bytes
       conformed 62 packets, 2866 bytes; actions
         transmit
       exceeded 0 packets, 0 bytes; actions:
         drop
       conformed 0 bps, exceed 0 bps

   Class-map: class-default (match-any)
     38 packets, 2944 bytes
     5 minute offered rate 0 bps, drop rate 0 bp
```



**NEW QUESTION: 329**

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

Which configuration meets this requirement at the hub router?

**A.** interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp map multicast dynamic
ip nbrp network-id 10
tunnel mode gre multipoint

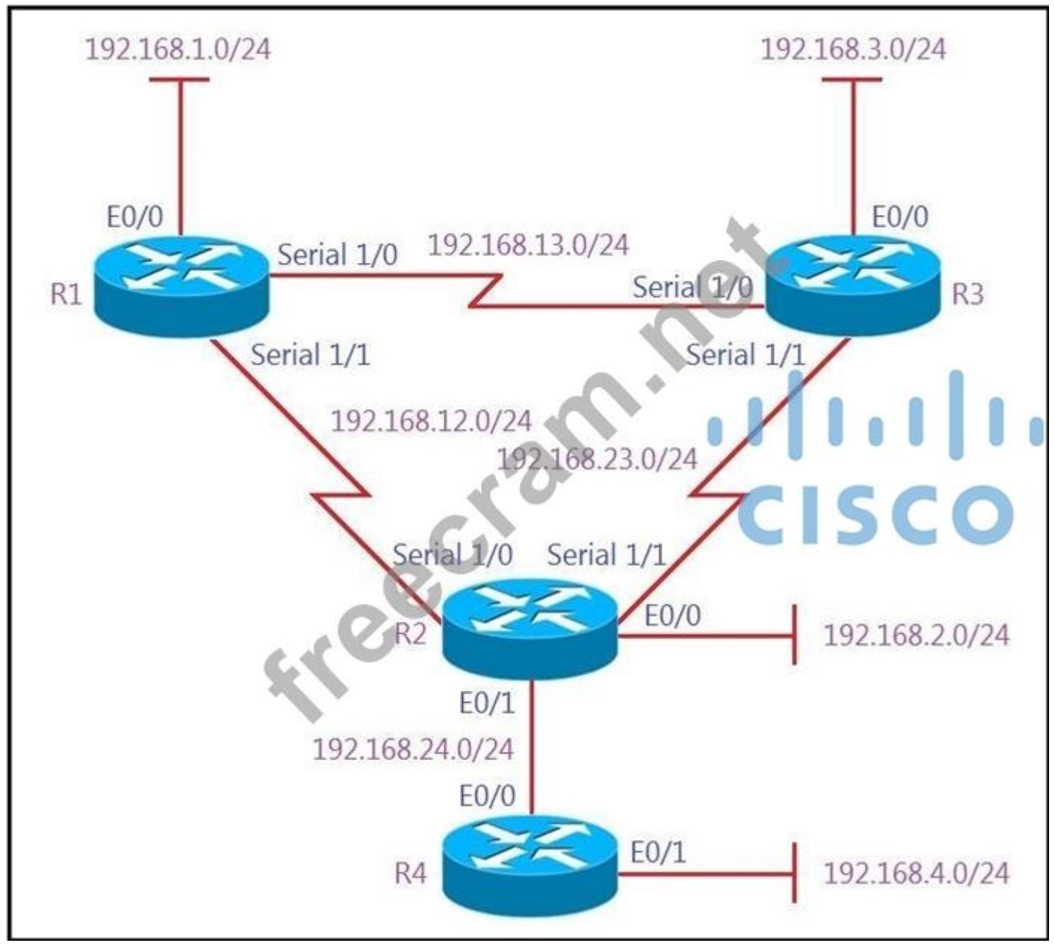
**B.** interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nbrp authentication KEY1
ip nhrp nhs dynamic ip nhop network-id 10
tunnel mode mgre auto

**C.** interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp map multicast 224.0.0.0
ip nhrp network-id 10
tunnel mode gre ipv4

**D.** interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1

ip nhrp registration no-unique
ip nhrp network-id 10
tunnel mode gre nmba
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 330**
Refer to the exhibit. All the serial between R1, R2, and R3 have the Same bandwidth. User on the
192.168.1.0/24 network report slow response times while they access resource on network
192.168.3.0/24. When a traceroute is run on the path. It shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 is still up.
What must the network administrator to fix the slowness?



```
# Show IP route on R1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/0
L        192.168.1.1/32 is directly connected, Ethernet0/0
D        192.168.2.0/24 [90/2297856] via 192.168.12.2, 00:02:14, Serial1/1
S        192.168.3.0/24 [1/0] via 192.168.12.2
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Serial1/1
L        192.168.12.1/32 is directly connected, Serial1/1
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/24 is directly connected, Serial1/0
L        192.168.13.1/32 is directly connected, Serial1/0
D        192.168.23.0/24 [90/2681856] via 192.168.13.3, 00:06:38, Serial1/0
                         [90/2681856] via 192.168.12.2, 00:06:38, Serial1/1
D        192.168.24.0/24 [90/2195456] via 192.68.12.2, 00:06:38, Serial1/1
```



**A.** Remove the static route on R1.
**B.** Redistribute the R1 route to EIGRP
**C.** Add a static route on R1 using the next hop of R3.
**D.** Change the Administrative Distance of EIGRP to 5.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 331**
Refer to the exhibit. The IP SLA probes 1, 2, and 3 verify the reachability of three distinct DNS servers hosted by ISP1. If all DNS servers are unreachable, the router should failover to ISP2 for Internet connectivity. However, the configuration is causing the router to failover to ISP2 even if some of the DNS servers are still reachable. Which action resolves the issue?

```
track 11 ip sla 1
!
track 12 ip sla 2
!
track 13 ip sla 3
!
track 14 list boolean and
 object 11
 object 12
 object 13
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 14
ip route 0.0.0.0 0.0.0.0 198.51.100.1 14 name ISP2
```



**A.** Use the administrative distance of 255 for the default route through ISP2.
**B.** Reference the track object 14 to the IP SLA probes 1, 2, and 3 directly.
**C.** Rewrite the track object 14 to use the "or" operator.
**D.** Use the delay command in the track object 14.
**Answer: (SHOW ANSWER)**
Currently, track 14uses the Boolean andoperator, meaning all three IP SLA objects (11, 12,
13) must be up for the route via ISP1 to stay active. If any one of them fails, the condition fails and the router incorrectly switches to ISP2.
To ensure the router only switches to ISP2 when all three probes fail, the trackobject should use the oroperator. This way, as long as at least one probe is successful, the route via ISP1 remains valid.



**NEW QUESTION: 332**
What are two functions of MPLS Layer 3 VPNs? (Choose two.)
**A.** LDP and BGP can be used for Pseudowire signaling.
**B.** It is used for transparent point-to-multipoint connectivity between Ethernet links/sites.
**C.** BGP is used for signaling customer VPNv4 routes between PE nodes.
**D.** A packet with node segment ID is forwarded along with shortest path to destination.
**E.** Customer traffic is encapsulated in a VPN label when it is forwarded in MPLS network.
**Answer: (SHOW ANSWER)**
MPLS Layer-3 VPNs provide IP connectivity among CE sites
MPLS VPNs enable full-mesh, hub-and-spoke, and hybrid IP connectivity
CE sites connect to the MPLS network via IP peering across PE-CE links
MPLS Layer-3 VPNs are implemented via VRFs on PE edge nodes
VRFs providing customer routing and forwarding segmentation

BGP used for signaling customer VPN (VPNv4) routes between PE nodes
To ensure traffic separation, customer traffic is encapsulated in an additional VPN label when forwarded in MPLS network
Key applications are layer-3 business VPN services, enterprise network segmentation, and segmented layer-3 Data Center access Reference:
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKMPL-1100.pdf

**NEW QUESTION: 333**
Refer to the exhibit. Router R2 VLAN 10 users cannot get dynamic IP addresses from R1. Which action resolves the issue?


```
R2#debug ip dhcp server events
000249: *Jun 19 02:13:33.818: DHCPD: Sending notification of DISCOVER:
000250: *Jun 19 02:13:33.823:   DHCPD: htype 1 chaddr 0c82.430d.db00
000251: *Jun 19 02:13:33.827:   DHCPD: remote id 020a0000c0a8000100000000
000252: *Jun 19 02:13:33.830:   DHCPD: circuit id 00000000
000253: *Jun 19 02:13:33.836: DHCPD: Seeing if there is an internally specified pool class:
000254: *Jun 19 02:13:33.840:   DHCPD: htype 1 chaddr 0c82.430d.db00
000255: *Jun 19 02:13:33.843:   DHCPD: remote id 020a0000c0a8000100000000
000256: *Jun 19 02:13:33.846:   DHCPD: circuit id 00000000
000257: *Jun 19 02:13:33.851: DHCPD: subnet [192.168.0.1,192.168.0.2] in address pool WAN is empty.
000258: *Jun 19 02:13:33.853: DHCPD: Sending notification of ASSIGNMENT FAILURE:
000259: *Jun 19 02:13:33.857:   DHCPD: htype 1 chaddr 0c82.430d.db00
000260: *Jun 19 02:13:33.861:   DHCPD: remote id 020a0000c0a8000100000000
000261: *Jun 19 02:13:33.865:   DHCPD: circuit id 00000000
000262: *Jun 19 02:13:33.870: DHCPD: Sending notification of ASSIGNMENT_FAILURE:
000263: *Jun 19 02:13:33.872:  DHCPD: due to: POOL EXHAUSTED
000264: *Jun 19 02:13:33.877:   DHCPD: htype 1 chaddr 0c82.430d.db00
000265: *Jun 19 02:13:33.879:   DHCPD: remote id 020a0000c0a8000100000000
000266: *Jun 19 02:13:33.879:   DHCPD: circuit id 00000000
000267: *Jun 19 02:13:36.860: DHCPD: Sending notification of DISCOVER:
000268: *Jun 19 02:13:36.862:   DHCPD: htype 1 chaddr 0c82.430d.db00
```

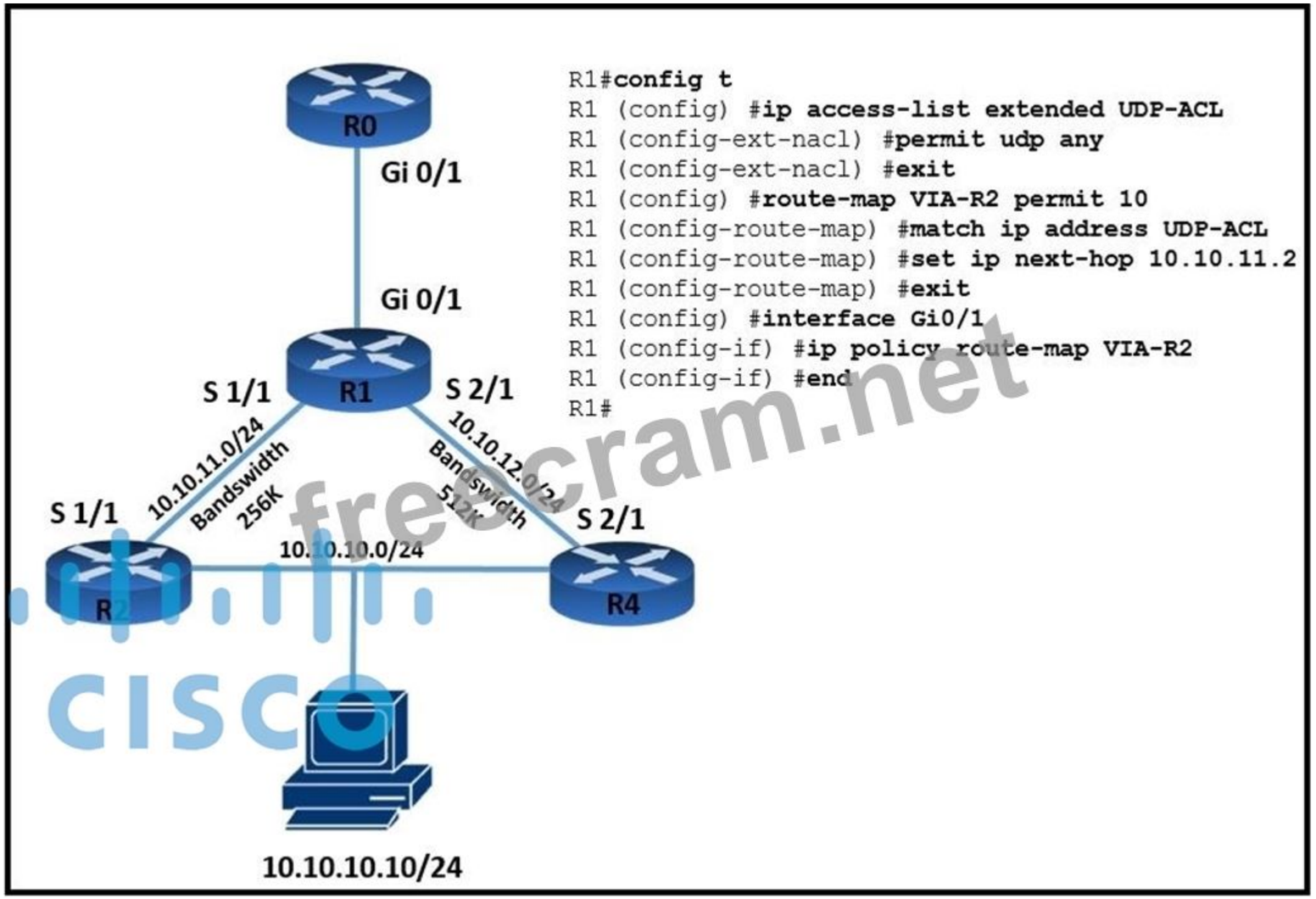
**A.** Identify the host with the duplicate IP address.
**B.** Expand the address scope of VLAN 10.
**C.** Eliminate the port security feature on the ports of switch SW2.
**D.** Configure the IP helper feature on the Interface GigabitEthernet 0/2 of router R2.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 334**

Refer to the exhibit. TCP traffic should be reaching host 10.10.10.10/24 via R2.

Which action resolves the issue?




**A.** TCP traffic will reach the destination via R2 without any changes

**B.** Add a permit 20 statement in the route map to allow TCP traffic

**C.** Allow TCP in the access list with no changes to the route map

**D.** Set IP next-hop to 10.10.12.2 under the route-map permit 10 to allow TCP traffic.

**Answer: (SHOW ANSWER)**

The ACL is for UDP only BUT is already forced through R2 to reach 10.10.10.10.

The BW is higher via R4 so that's the path TCP will take, so adding the TCP to the ACL forces it also via R2.

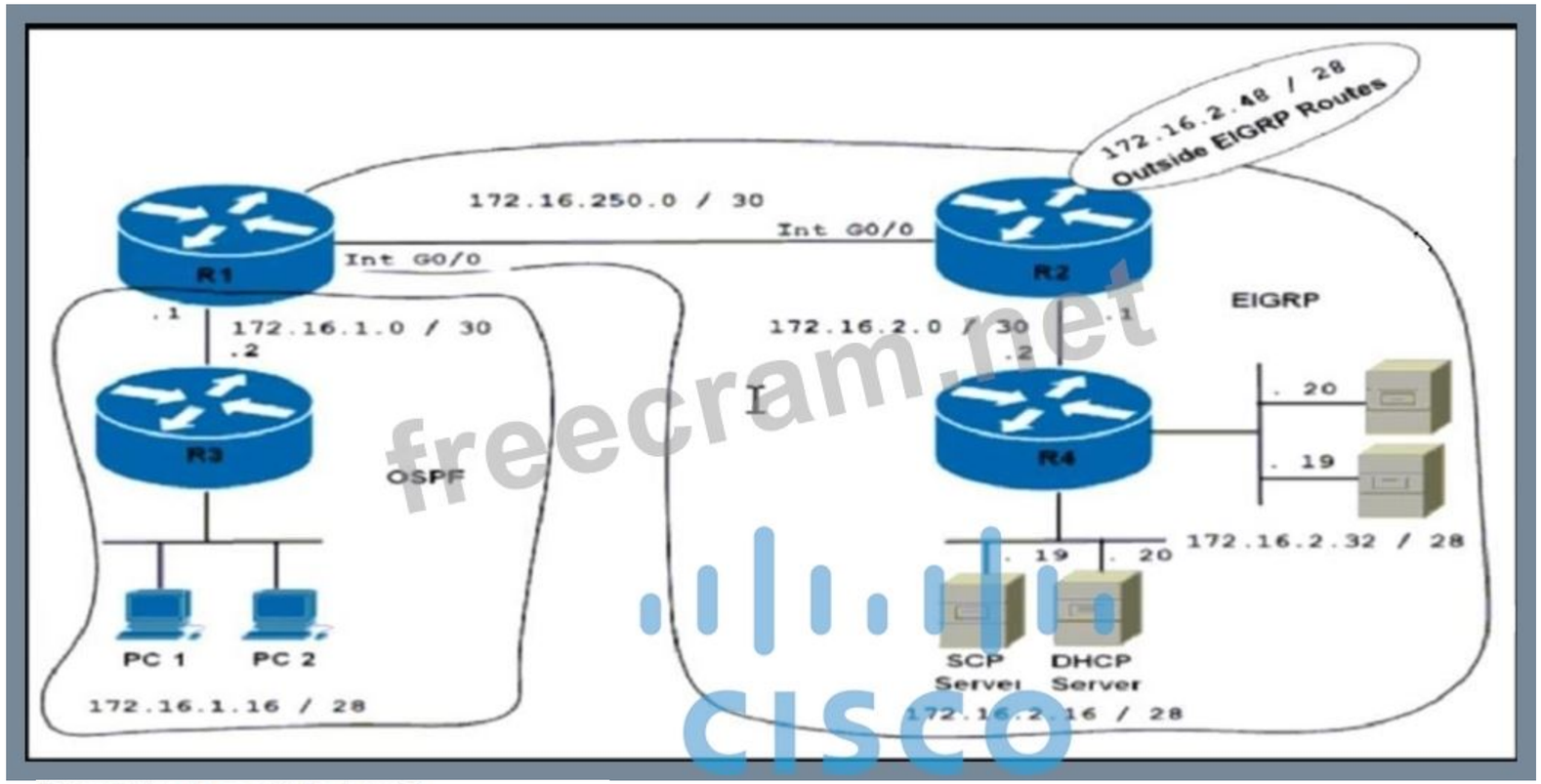
**NEW QUESTION: 335**

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

```
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#
```






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-2
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
```

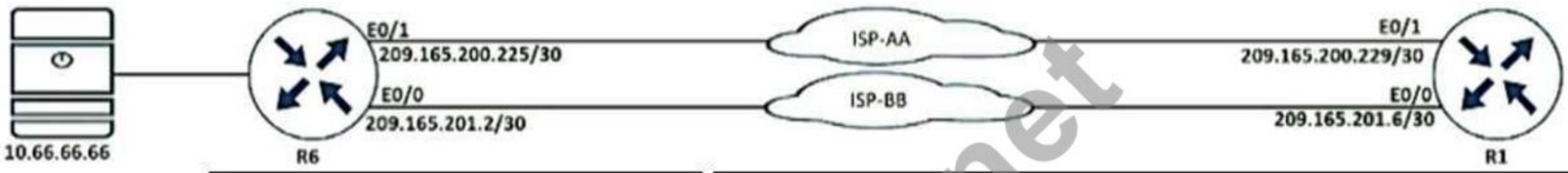
C.
```
R1(config)#route-map CCNP deny 10
R1(config-route-map)#no match route-type local
R1(config-route-map)#match route-type external  type-1
R1(config)#route-map CCNP permit 20
```

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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 336**

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?



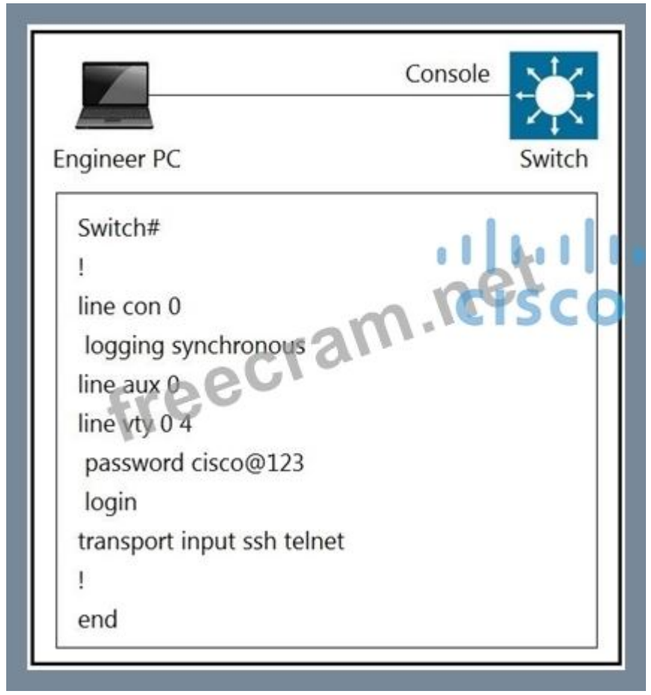

```
R1#
ip route 10.66.66.0 255.255.255.0 10.2.2.4 track 700
ip route 10.66.66.0 255.255.255.0 10.1.1.3 20
!
track 700 ip sla 700
!
ip sla 700
 icmp-echo 10.66.66.66 source-ip 10.10.10.1
 threshold 100
 frequency 5
ip sla schedule 700 life forever start-time now
```

```
R1#
*Nov 18 15:38:59.956: track-sta (700) Change #8 ip sla 700, state Up->Down
*Nov 18 15:38:59.956: %TRACK-6-STATE: 700 ip sla 700 state Up -> Down
*Nov 18 15:38:59.956: track-sta (700) ip sla 700 state Up -> Down
*Nov 18 15:38:59.956: track-que (700) Queuing CHANGED client event for Static IP Routing
*Nov 18 15:38:59.956: track-que (700) Unqueuing CHANGED client event for Static IP Routing
*Nov 18 15:39:04.965: track-sta (700) Change #9 ip sla 700, state Down->Up
*Nov 18 15:39:04.965: %TRACK-6-STATE: 700 ip sla 700 state Down -> Up
*Nov 18 15:39:04.965: track-sta (700) ip sla 700 state Down -> Up
*Nov 18 15:39:04.965: track-que (700) Queuing CHANGED client event for Static IP Routing
*Nov 18 15:39:04.966: track-que (700) Unqueuing CHANGED client event for Static IP Routing
```

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

ID        Type        Destination       Stats       Return      Last
                                        (ms)        Code        Run
---------------------------------------------------------------------
*700      icmp-echo   10.66.66.66       RTT=1       OK          4 seconds ago
```

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

**NEW QUESTION: 337**
Refer to the exhibit. An engineer must block access to the console ports for all corporate remote Cisco devices based on the recent corporate security policy but the security team stilt can connect through the console port. Which configuration on the console port resolves the issue?





**A.** transport input telnet
**B.** login and password
**C.** no exec
**D.** exec 0.0
**Answer: (SHOW ANSWER)**
When you want to allow an outgoing connection only for a line (no incoming) use the no exec command. When a user tries to Telnet to a line with the no exec command configured, the user will get no response when pressing the Return key at the login screen.

**NEW QUESTION: 338**
Which Layer 3 VPN attribute allows different customers to connect to the same MPLS network with overlapping IP ranges?
**A.** RT
**B.** MP-BGP
**C.** VRF
**D.** RD
**Answer: (SHOW ANSWER)**

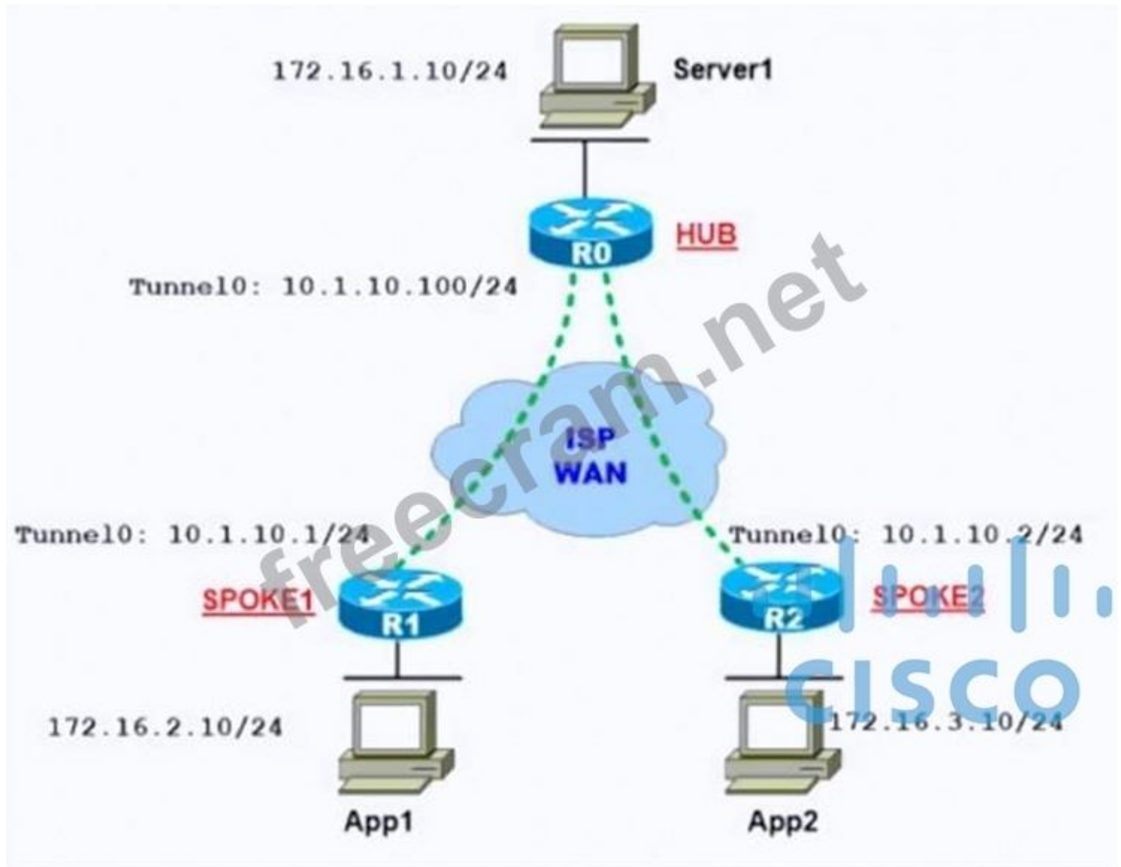
**NEW QUESTION: 339**
Refer to the exhibit. An administrator can log in to the device using Telnet, but the attempts to log in to the same device using SSH with the same credentials fail. Which action resolves this issue?

```
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:~$
```



**A.** Configure to use the Telnet user database for SSH as well.
**B.** Configure SSH service on the router.
**C.** Configure transport input all on the VTY lines to allow SSH.
**D.** Configure the VTY lines with login local.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 340**
Refer to the exhibit. An engineer must establish optimal routing between the app servers connected at the SPOKE routers. Which configurations are required on each router to create a distributed mapping database between SPOKE1 and SPOKE2 to achieve optimal routing so the traffic is forwarded directly from the App1 server to the App2 server?



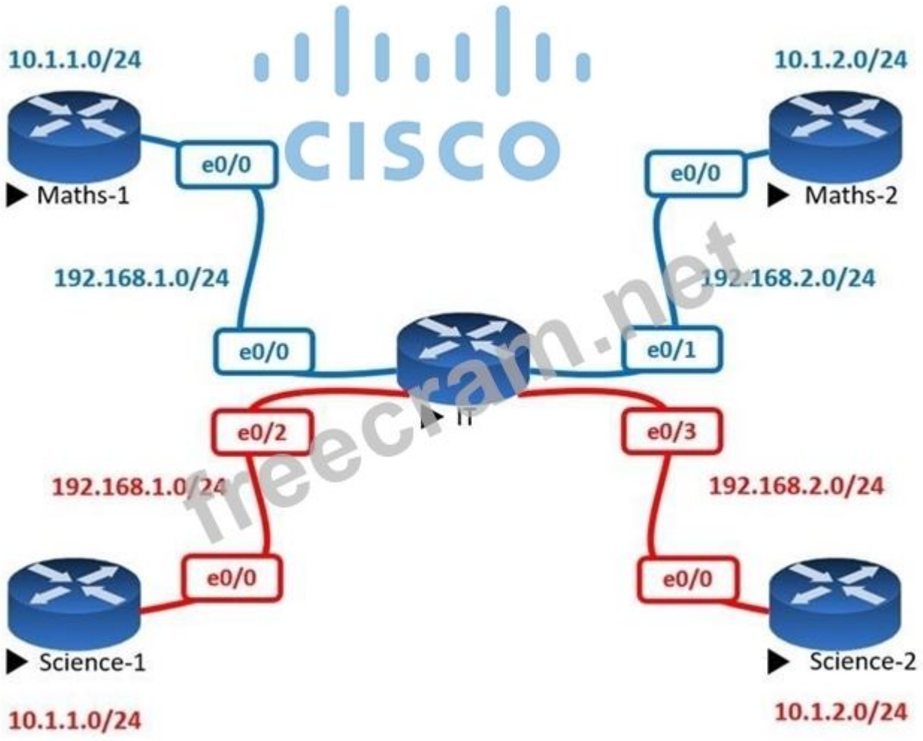



**A.** R0#
interface Tunnel0
tunnel mode gre multipoint
ip nhrp redirect
R1#
interface Tunnel0
tunnel mode gre multipoint
ip nhrp shortcut
R2#
interface Tunnel0
tunnel mode gre multipoint
ip nhrp shortcut

**B.** R0#
interface Tunnel0
tunnel mode dvmrp
ip nhrp shortcut
R1#

interface Tunnel0
tunnel mode dvmrp
ip nhrp redirect
R2#
interface Tunnel0
tunnel mode dvmrp
ip nhrp redirect
**C.** R0#
interface Tunnel0
tunnel mode dvmrp
ip nhrp redirect
R1#
interface Tunnel0
tunnel mode dymrp
ip nhrp shortcut
R2#
interface Tunnel0
tunnel mode dvmrp
ip nhrp shortcut
**D.** R0#
interface Tunnel0
tunnel mode gre multipoint
ip nhrp shortcut
R1#
interface Tunnel0
tunnel mode gre multipoint
ip nhrp redirect
R2#
interface Tunnel0
tunnel mode gre multipoint
ip nhrp redirect
**Answer: (SHOW ANSWER)**
The hub must be configured with ip nhrp redirect to notify the spokes of optimal routing paths.
tunnel mode gre multipoint is required for DMVPN. The spokes must be configured with ip nhrp shortcut to support direct spoke-to-spoke communication. tunnel mode gre multipoint is also necessary. This setup ensures optimal routing with direct spoke-to-spoke communication.

**NEW QUESTION: 341**
Refer to the exhibit. The Math and Science departments connect through the corporate IT router but users in the Math department must not be able to reach the Science department and vice versa Which configuration accomplishes this task?




A.

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

B.

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

C.

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

D.

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

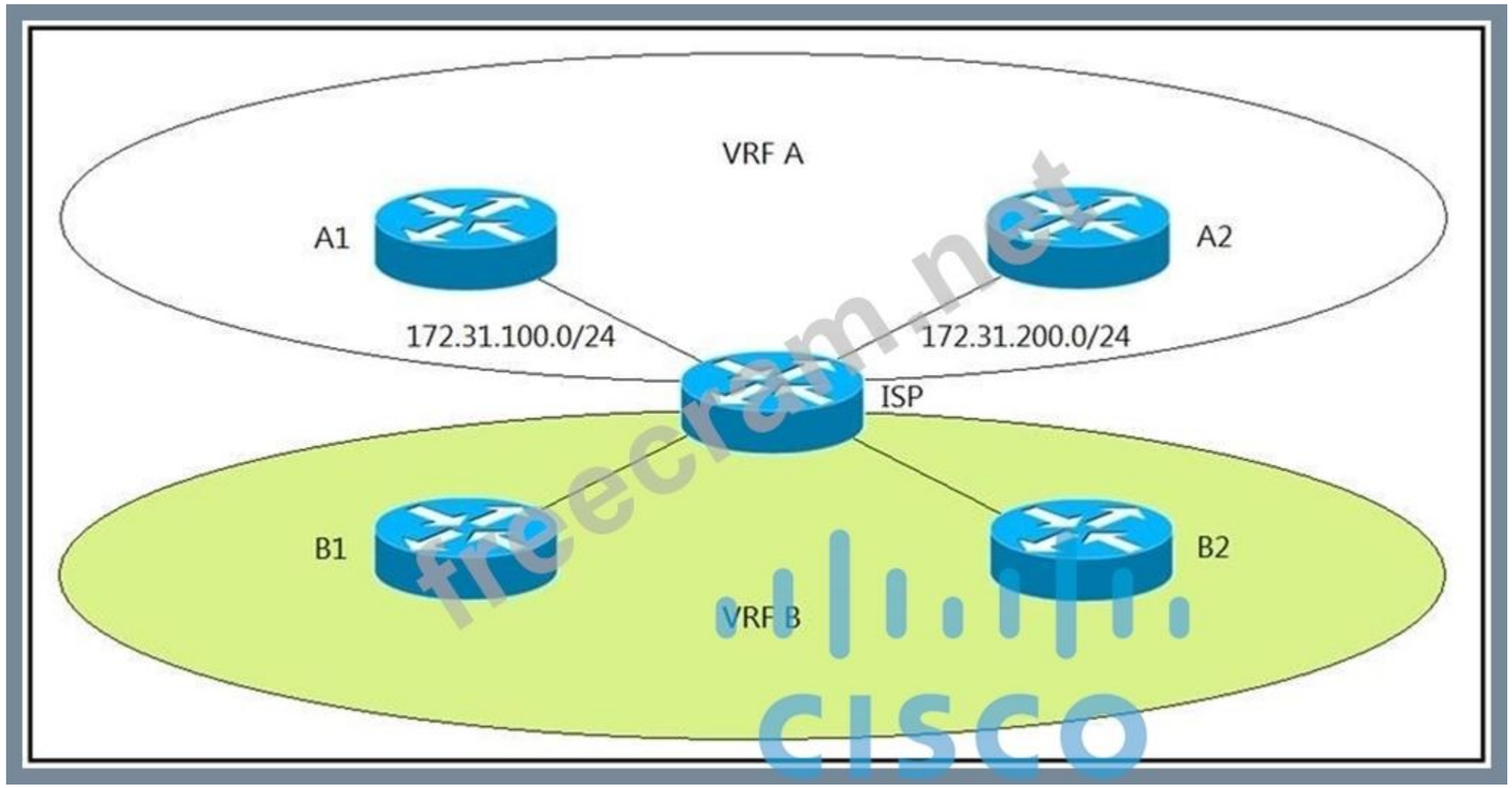
**Answer: (SHOW ANSWER)**

```
ISP(config)#interface FastEthernet 0/0
ISP(config-if)#ip vrf forwarding Blue
% Interface FastEthernet0/0 IP address 192.168.1.254 removed due to enabling VRF Blue
ISP(config-if)#ip address 192.168.1.254 255.255.255.0
```

On the interface level we use the **ip vrf forwarding command** to assign the interface to the correct VRF. Once you do this , you'll have to add the IP address again. Let's configure the remaining interfaces:

```
ISP(config)#interface FastEthernet 1/0
ISP(config-if)#ip vrf forwarding Red
ISP(config-if)#ip address 192.168.2.254 255.255.255.0

ISP(config)#interface FastEthernet 2/0
ISP(config-if)#ip vrf forwarding Blue
ISP(config-if)#ip address 192.168.3.254 255.255.255.0
```

**NEW QUESTION: 342**
Refer to the exhibit. The ISP router is fully configured for customer A and customer B using the VRF- Lite feature.
What is the minimum configuration required for customer A to communicate between routers A1 and A2?




**A.** A1:
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100 vrf A
net 172.31.100.1 0.0.0.255 area 0
A2:
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100 vrf A
net 172.31.200.1 0.0.0.255 area 0
**B.** A1:

interface fa0/0
description To->ISP
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
A2:
interface fa0/0
description To->ISP
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
**C.** A1:
interface fa0/0
description To->ISP
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
A2:
interface fa0/0
description To->ISP
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
**D.** A1:
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
A2:

interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 343**
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.
The set ip next-hop command verifies the existence of the next hop specified, and... If the next hop exists in the routing table, then the command policy routes the packet to the next hop.
- If the next hop does not exist in the routing table, the command uses the normal routing table to forward the packet.
Reference: https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds- ce.html

**NEW QUESTION: 344**
Which type of ports are protected by IPv6 Source Guard?
**A.** Layer 2 ports
**B.** access ports
**C.** Layer 3 ports
**D.** trunk ports
**Answer: (SHOW ANSWER)**
IPv6 Source Guard is a security feature that helps protect the network from IPv6 address spoofing by ensuring that only specific, valid IPv6 addresses can be used on a given port.
IPv6 Source Guard typically works on access ports. These are ports where devices are connected that are typically assigned specific IPv6 addresses (such as end-user devices).
Access ports carry traffic for a single VLAN, and Source Guard ensures that only authorized IPv6 addresses can be used on those ports.

**NEW QUESTION: 345**
The OSPF dead interval defaults to how many times the hello interval?
**A.** Three
**B.** Four
**C.** Five

**D.** Two
**Answer: (SHOW ANSWER)**

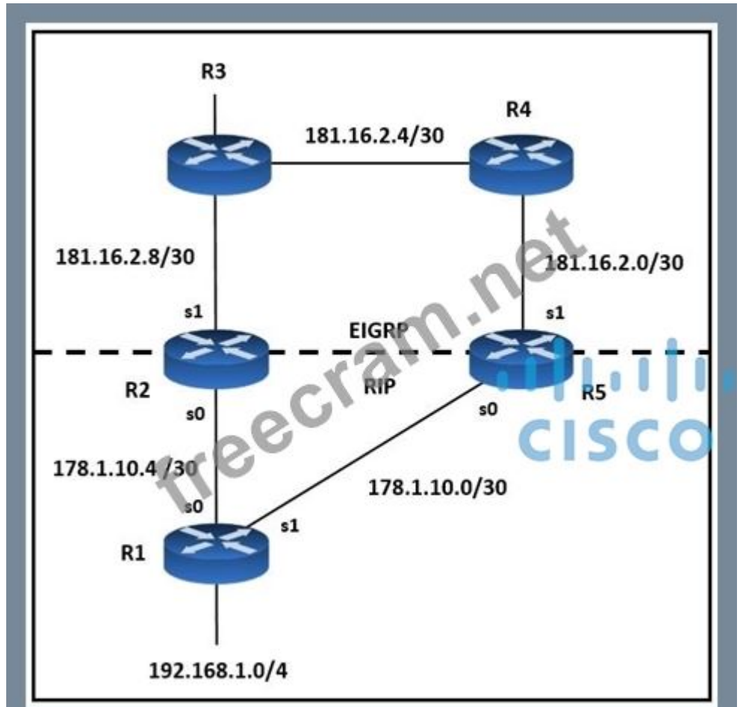
**NEW QUESTION: 346**
Refer to the exhibit. Which action resolves the issue?

```
R1(config)# ip access-list extended CoPP-4_OSPF
R1(config-ext-nacl)# permit ospf any host 224.0.0.5 log
R1(config-ext-nacl)# permit ospf any host 224.0.0.6 log-input
R1(config-ext-nacl)# end
```

**A.** Resolve the misconfigured QoS parameters.
**B.** Replace the faulty cable.
**C.** Upgrade the hardware to increase the interface input buffers.
**D.** Implement traffic policing to prevent the interface input traffic being exceeded.
**Answer: D (LEAVE A REPLY)**
CoPP protects the control plane of a router by managing the rate at which control traffic is allowed to reach the CPU. In this case, OSPF traffic directed to multicast addresses 224.0.0.5 and 224.0.0.6 is being logged and processed by the control plane.
The log and log-input keywords in the ACL result in additional CPU utilization to generate log messages for every matching packet. This can overload the control plane when large amounts of OSPF traffic are received.
By implementing traffic policing, you can limit the rate of incoming control plane traffic to ensure it does not exceed the available interface input buffer or overwhelm the router's CPU.



**NEW QUESTION: 347**
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?

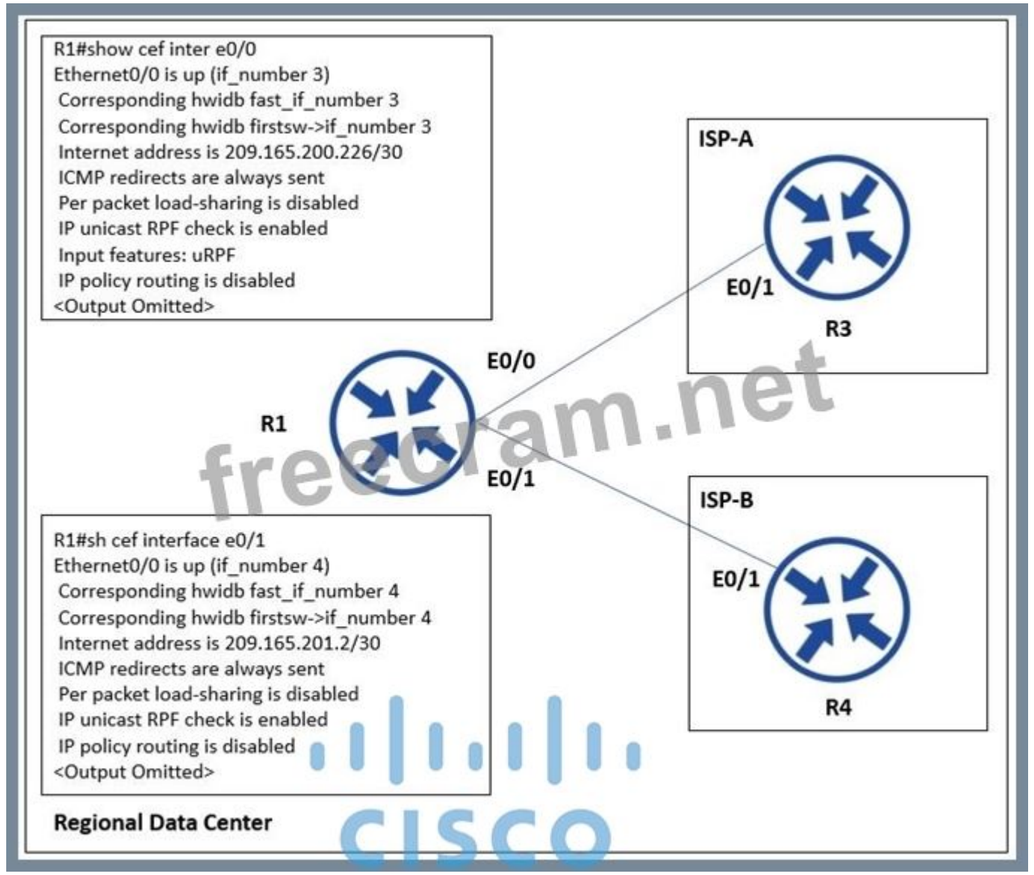



**A.** R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list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

!
access-list 1 deny 192.168.1.0
access-list 1 permit any
**B.** R2:
router eigrp 7
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 7 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 7
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 7 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
**C.** R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10

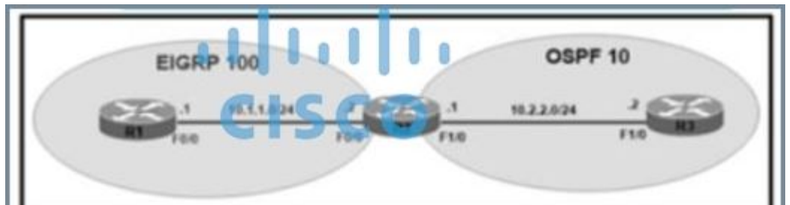
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
**D.** R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 348**
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.** interface ethernet0/1
ip verify unicast reverse-path
**B.** interface ethernet0/0
ip unicast RPF check reachable-via any allow-default allow-self-ping
**C.** interface ethernet0/0
ip verify unicast reverse-path
**D.** interface ethernet0/1
ip unicast RPF check reachable-via any allow-default allow-self-ping
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 349**
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?




**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



**A.** passive-interface FastEthernet 0/0 command in OSPF1.
**B.** Add the no auto-summary command in EIGRP 100.
**C.** Replace the network 10.0.0.0 command with FastEthernet0/0 network in EIGRP 100.
**D.** Add the passive-interface FastEthernet 1/0 command in EIGRP 100.
**Answer: (SHOW ANSWER)**
Making FastEthernet1/0 passive in EIGRP would prevent EIGRP from forming neighbor relationships or advertising routes over that interface. This would isolate the 10.2.2.0/24 network from EIGRP, effectively preventing the OSPF route from leaking into EIGRP on R1. This configuration would stop the unexpected routing information from propagating between OSPF and EIGRP.

**NEW QUESTION: 350**
What is a function of BFD?
**A.** peer recovery after a Layer 3 protocol adjacency failure
**B.** peer recovery after a Layer 2 adjacency failure
**C.** failure detection independent of routing protocols and media types
**D.** failure detection dependent on routing protocols and media types
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 351**
Refer to the exhibit. Which action resolves the issue?

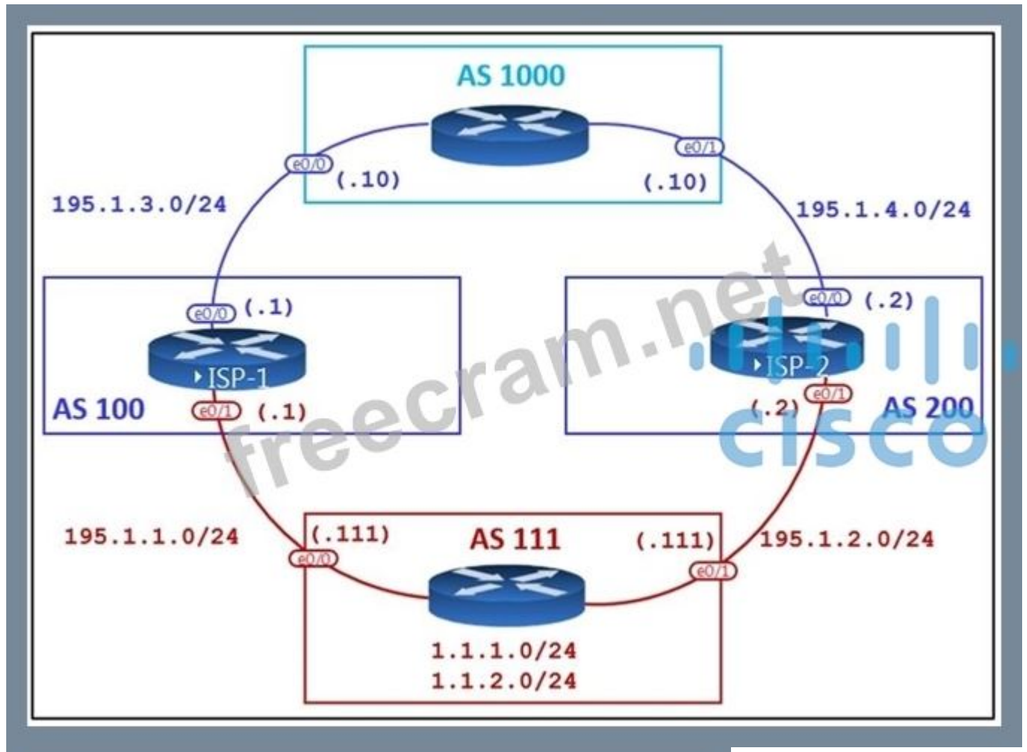
```
March 10 19:28:53.254 GMT: %SNMP-3-AUTHFAIL: Authentication
failure for SNMP request from host 10.1.1.1

snmp-server community public RO 15
snmp-server community private RW 16
!
logging snmp-authfail
!
access-list 15 permit 10.1.1.1

access-list 16 permit 10.1.1.2
```



**A.** Configure host IP address in access-list 16.
**B.** Configure SNMPv3 on the router.
**C.** Configure SNMP authentication on the router.
**D.** Configure a valid SNMP community string.
**Answer: (SHOW ANSWER)**
Looking at the configuration, it seems that there are two SNMP community strings configured,
"public" and "private". However, the configuration does not specify which community string is being used by the host with IP address 10.1.1.1.
The correct action to resolve this issue would be to configure a valid SNMP community string on the device from which the SNMP request is being made, and ensure that it matches the community string configured on the router.

**NEW QUESTION: 352**
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 the input-queue command to prevent the loss of packets.
**C.** Use WFQ in the output queue of the high-performance router.
**D.** Use RIP V2 to be able to use classless networks from BGP
**Answer: D (LEAVE A REPLY)**
RIP Version 1 (RIP V1) only supports classful routing, meaning it does not carry subnet mask information in its updates. As a result, when BGP routes (which are often classless) are redistributed into RIP V1, they may be misinterpreted or discarded due to the lack of subnet mask information.
To resolve the issue, switch to RIP V2, which supports classless routing and includes subnet mask information in its updates. This ensures that classless BGP routes can be correctly redistributed and propagated in the RIP network.

**NEW QUESTION: 353**
Refer to the exhibit. AS111 is receiving its own routes from AS200 causing a loop in the network.



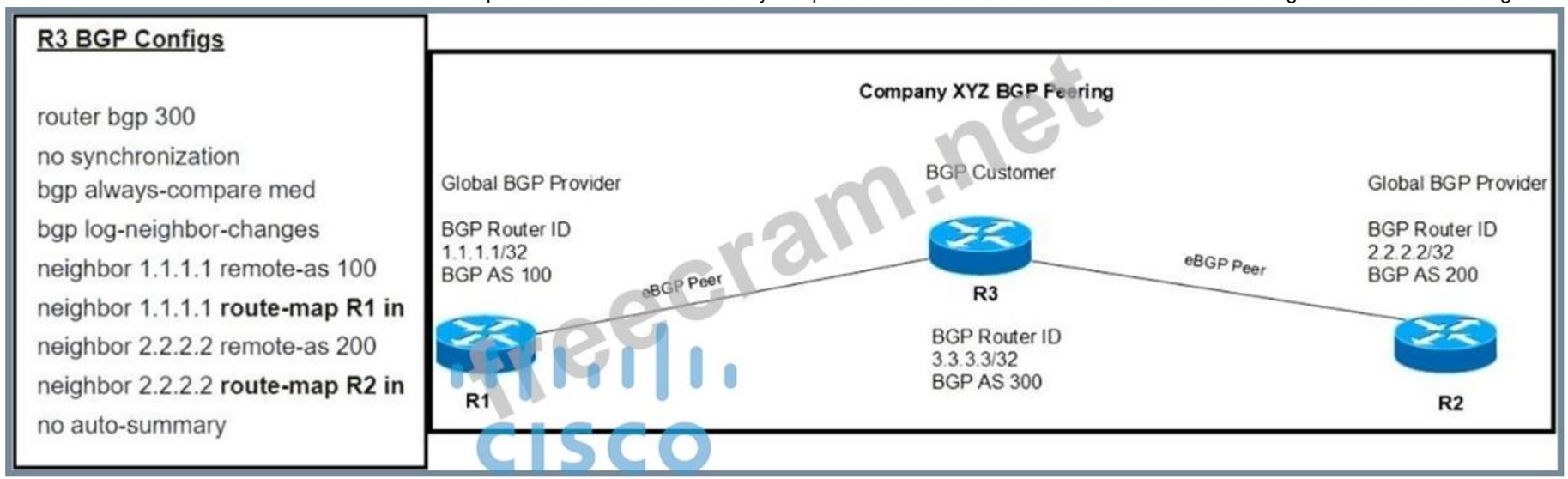

**AS111**

```
Router bgp 111
  Neighbor 195.1.1.1 remote-as 100
  Neighbor 195.1.1.1 allowas-in
  Neighbor 195.1.2.2 remote-as 200
  Neighbor 195.1.2.2 allowas-in
```

**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: (SHOW ANSWER)**
In this case, allow as-in is not needed because it disables control of AS_PATH. Allow as-in is the most logical explanation to this question.

**NEW QUESTION: 354**
Refer to the exhibit. R3 is dual-homed to two service providers for traffic redundancy. R3 prefers its outbound traffic via R2. Which set of configurations achieves this goal?




**A.** route-map R1 permit 10
set AS-Path Prepend 100
!
route-map R2 permit 10
set AS-Path Prepend 200
**B.** route-map R1 permit 10
set metric 100
!
route-map R2 permit 10
set metric 200
**C.** route-map R1 permit 10
set AS-Path Prepend 200
!
route-map R2 permit 10
set AS-Path Prepend 100
**D.** route-map R1 permit 10
set metric 200
!
route-map R2 permit 10
set metric 100
**Answer: (SHOW ANSWER)**

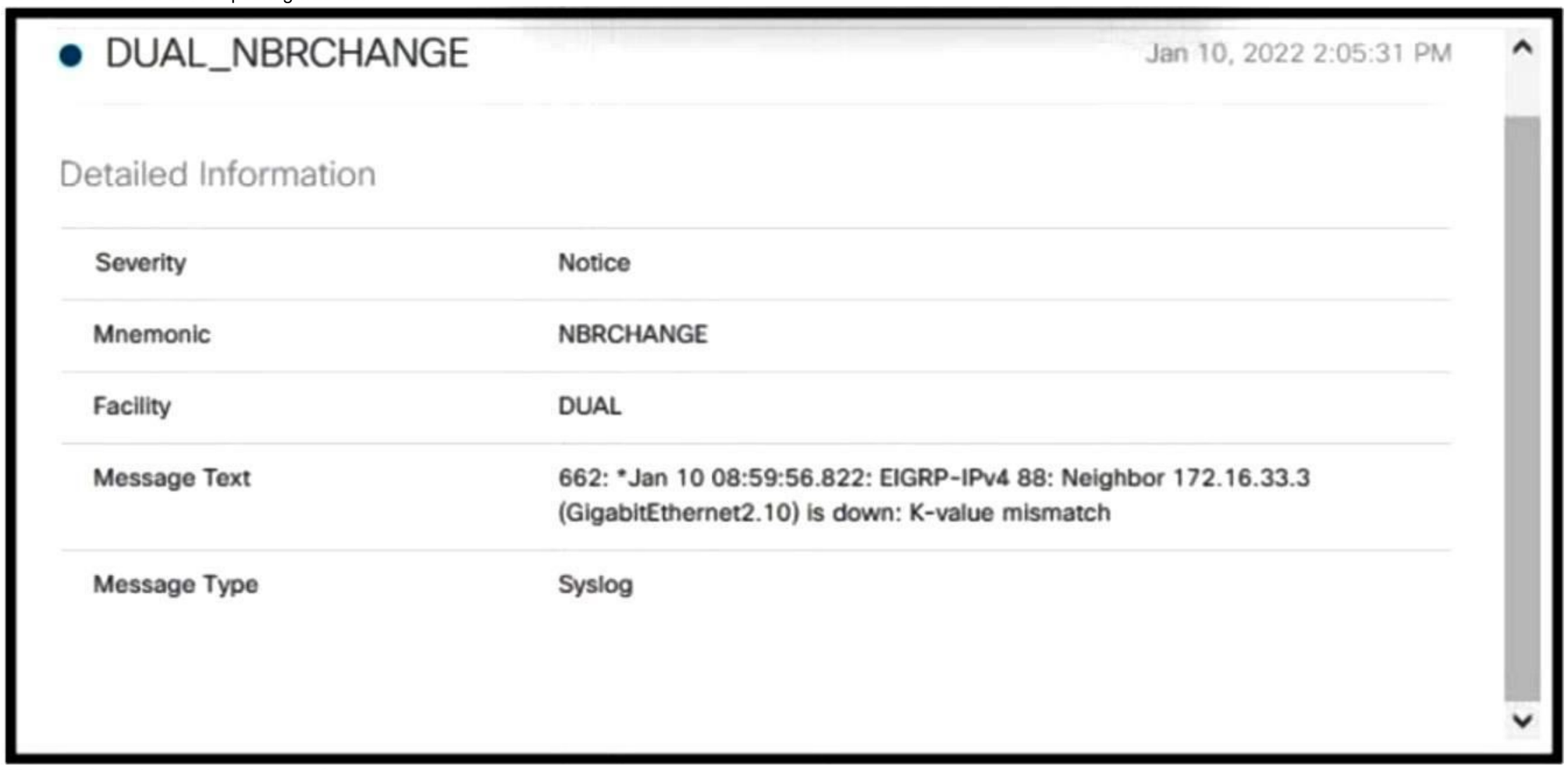
AS-path prepending allows you to artificially increase the length of the AS path for a specific neighbor, making that path less preferred in the BGP best-path selection process.
By prepending the AS-path for routes learned from R1 (with AS 200), you make routes via R1 less attractive.
Conversely, not prepending the AS-path for R2 (or prepending a smaller number, as done here) ensures that R3 prefers outbound traffic via R2, since the AS-path will be shorter.
R1's path will appear longer (with AS-path 200), so R3 will prefer sending traffic via R2.
Other options either do not prepend the AS-path correctly or adjust metrics that aren't optimal for BGP path preference in this context.

**NEW QUESTION: 355**
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 not showing R2 as a successor. Which action resolves the issue?

```
R1# show ip int br | ex una
Interface              IP-Address      OK? Method  Status                Protocol
Ethernet1/0            203.0.113.1     YES manual  up                    up
Loopback1              172.16.50.1     YES manual  up                    up
Loopback2              172.16.100.1    YES manual  up                    up
Loopback3              172.16.150.1    YES manual  up                    up

R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                          (sec)         (ms)       Cnt Num
0 203.0.113.2             Et1/0 14 00:31:16  1018  5000  0  24

R1# show ip eigrp topo all-links
EIGRP-IPv4 Topology Table for AS(1)/ID(172.16.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 409600, serno 34
        via 203.0.113.2 (409600/128256), Ethernet1/0
P 172.16.100.0/24, 1 successors, FD is 128256, serno 32
        via Connected, Loopback2
P 192.168.30.0/24, 1 successors, FD is 409600, serno 36
        via 203.0.113.2 (409600/128256), Ethernet1/0
P 203.0.113.0/24, 1 successors, FD is 281600, serno 33
        via Connected, Ethernet1/0
P 172.16.150.0/24, 1 successors, FD is 128256, serno 31
        via Connected, Loopback3
P 172.16.50.0/24, 1 successors, FD is 128256, serno 30
        via Connected, Loopback1
P 192.168.20.0/24, 1 successors, FD is 409600, serno 35
        via 2030.113.2 (409600/128256), Ethernet1/0
```

**A.** Resolve the incorrect metric on the link.
**B.** Enable split-horizon.
**C.** Configure the network statement on the neighbor.
**D.** Rectify the incorrect router ID in R2.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 356**
Refer to the exhibit. EIGRP peering was lost.




Which configuration resolves the issue?

**A.**
```
router EIGRP 88
 metric weights  1 0 1 0 10
```

**B.**
```
router EIGRP 88
 metric weights 0 1 1 0 01
```

**C.**
```
router EIGRP 88
 metric weights 0 1 1 1 0 0
```

```
router EIGRP 88
 metric weights 1 1 1 0 0 0
```

**D.**

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 357**

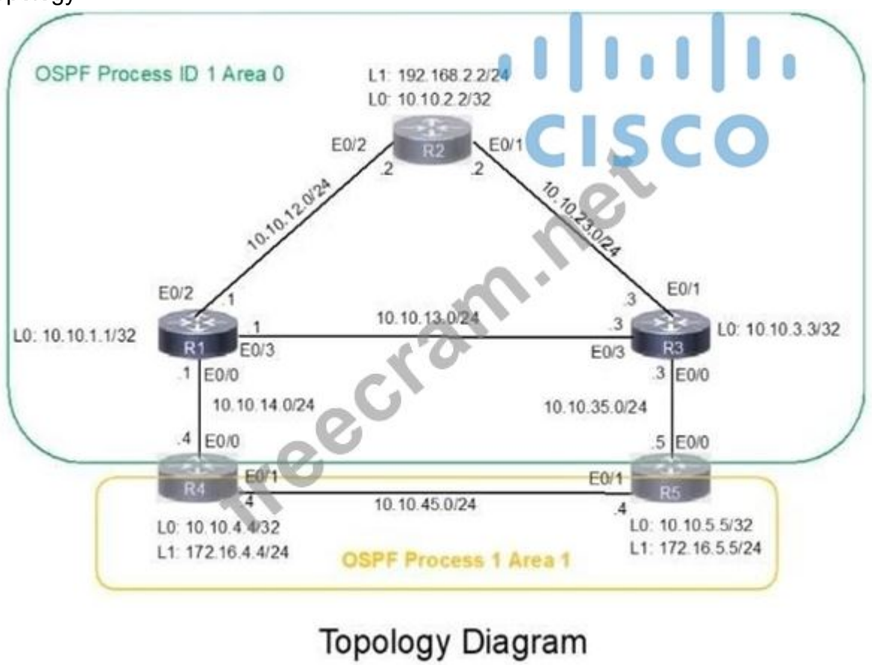
LAB SIMULATION 3

Guidelines

This is a lab item in which tasks will be performed on virtual devices.

* Refer to the Tasks tab to view the tasks for this lab item.
* Refer to the Topology tab to access the device console(s) and perform the tasks.
* Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
* All necessary preconfigurations have been applied.
* Do not change the enable password or hostname for any device.
* Do not replace existing routing policies or configurations.
* Save your configurations to NVRAM before moving to the next item.
* Click Next at the bottom of the screen to submit this lab and move to the next question.
* When Next is clicked, the lab closes and cannot be reopened.

Topology




Topology Diagram

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

```
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
!
!
!
```



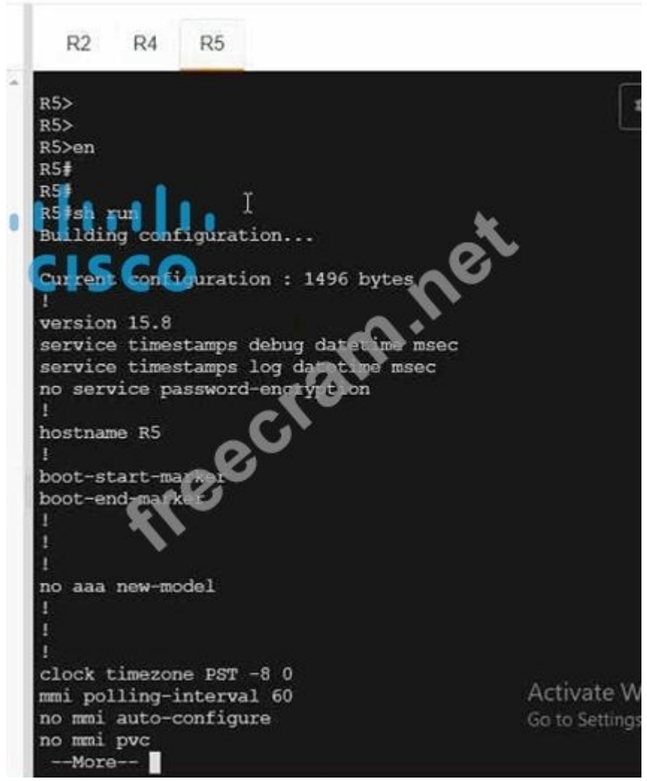
R4


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--
freecram.net
CISCO

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
CISCO
!
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
line aux 0
freecram.net
Activate W
Go to Settings
R5

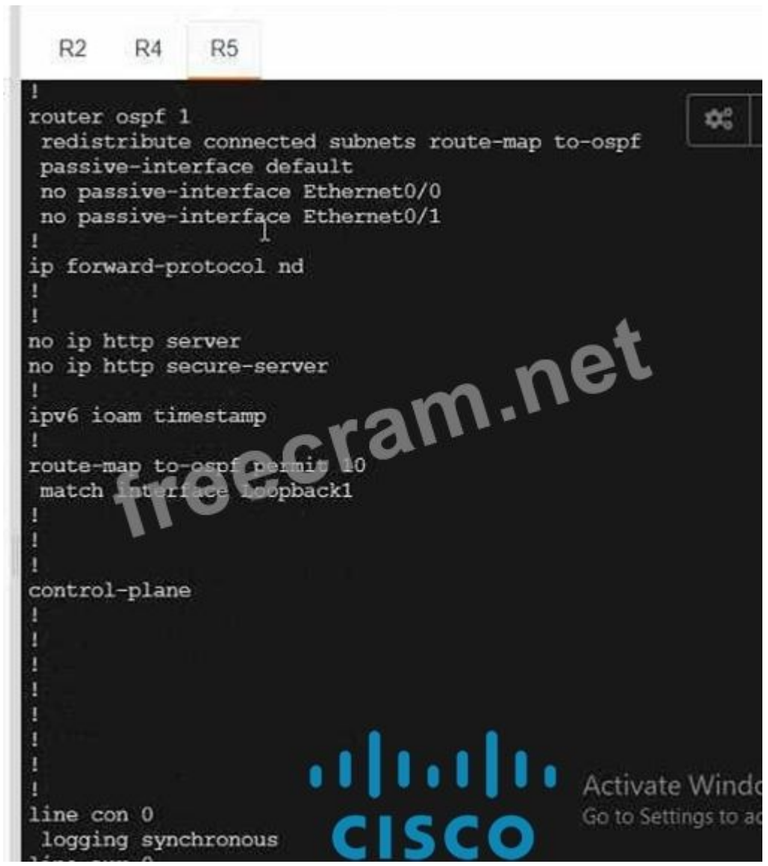


R2 R4 R5

```
!
!
!
!
!
!
!
!
!


!
!
!
!
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 10.10.35.5 255.255.255.0
 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:**

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

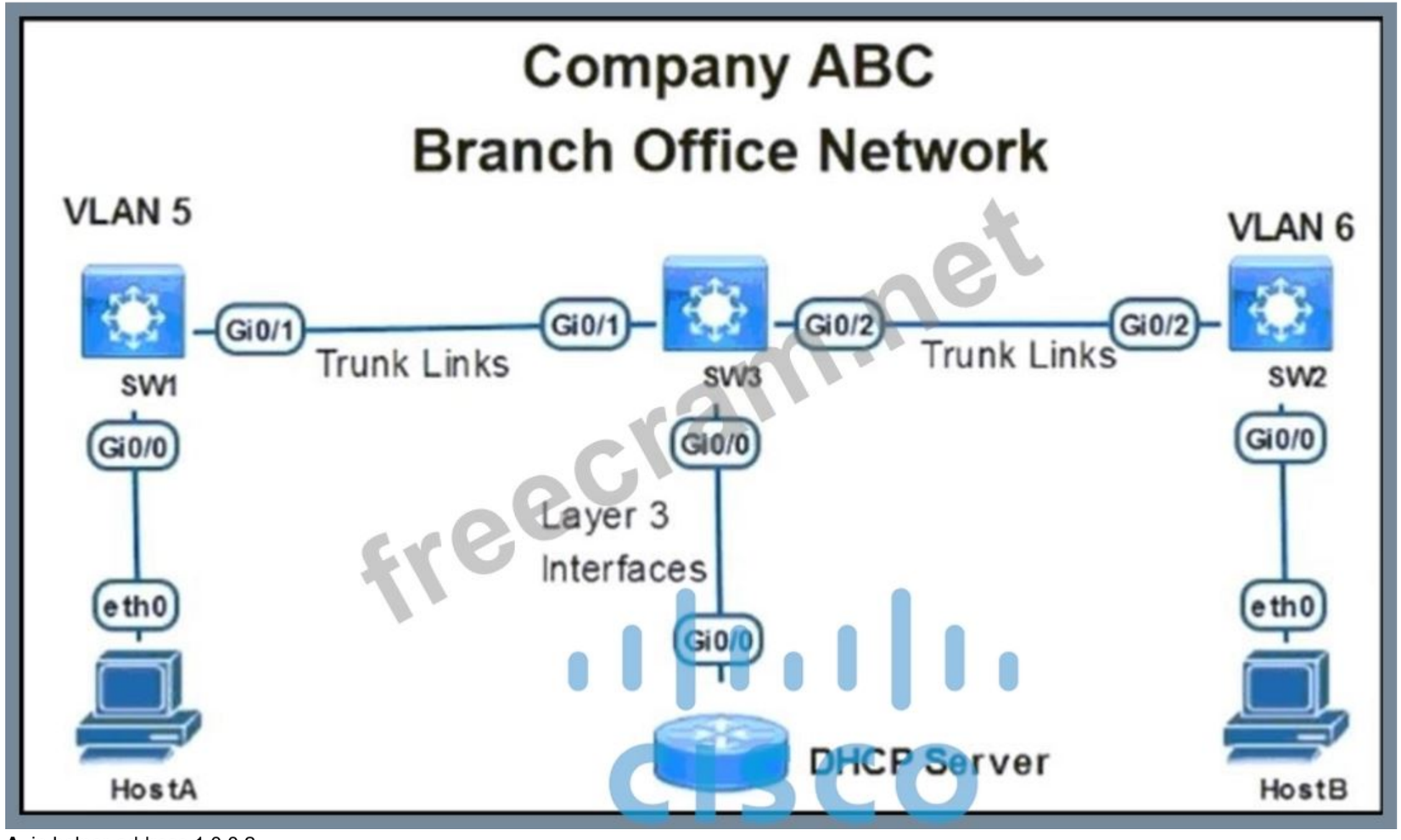
Copy run start

VERIFICATION:-

```
R2#show ip ospf nei
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         I
nterface
10.10.1.1         1   FULL/BDR        00:00:38    10.10.12.1      E
thernet0/2
10.10.3.3         1   FULL/BDR        00:00:30    10.10.23.3      E
thernet0/1
R2#
```



**NEW QUESTION: 358**
Refer to the exhibit. HostA and HostB cannot receive IP addresses from the DHCP server. The switches are configured with the DHCP snooping. Which configuration on SW3 resolves the issue?




**A.** ip helper-address 1.0.0.2
**B.** ip dhcp server use subscriber-id client-id
**C.** no ip dhcp snooping information option
**D.** ip dhcp relay information option-insert

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 359**
An engineer is trying to copy an IOS file from one router to another router by using TFTP.
Which two actions are needed to allow the file to copy? (Choose two.)
**A.** Configure the TFTP authentication on the source router with the tftp-server authentication local command.
**B.** Configure a user on the source router with the username tftp password tftp command.
**C.** Enable the TFTP server on the source router with the tftp-server flash:<filename> command.
**D.** TFTP is not supported in recent IOS versions, so an alternative method must be used.
**E.** Copy the file to the destination router with the copy tftp: flash: command
**Answer: (SHOW ANSWER)**
Below are the steps to follow for copying the Cisco IOS software image from a router acting as TFTP server to another router.
1. Check the image size on Router1 with the show flash command.
2. Check the image size on Router2 with the show flash command to verify if enough space is available on Router2 for the system image file to be copied.
3. Configure Router1 as the TFTP server: Router1(config)#tftp-server flash:/c2500-js-l.122-10b
4. When the TFTP server is configured, download the specified image from Router1 to Router2 using the copy tftp flash command.
Reference: https://www.cisco.com/c/en/us/support/docs/routers/2500-series-routers/15092- copyimage.html

**NEW QUESTION: 360**
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
router eigrp 100
```

**B.**
```
router ospf 1
    redistribute ospf 1 metric 10 10 10 10 10
```

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

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

**D.**

**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: 361**

Which two NLRI attributes are used by an MPLS Layer 3 VPN network to exchange VPNv4 routes between MPLS routers via MP-BGP? (Choose two.)

**A.** VPNv4 Prefix

**B.** Next Hop

**C.** Extended-Community

**D.** IPv4 Prefix

**E.** RT

**Answer: (SHOW ANSWER)**

How do we advertise these VPNv4 routes? That's what we need MP-BGP for.

MP-BGP supports IPv4 unicast/multicast, IPv6 unicast/multicast and it has support for VPNv4 routes. To exchange VPNv4 routes, MP-BGP uses a new NLRI (Network Layer Reachability Information) format that has the following attributes:

- RD (Route Distinguisher)
- IPv4 prefix
- Next Hop
- VPN Label

This is how PE routers exchange VPNv4 routes with each other.



**NEW QUESTION: 362**

Refer to the exhibit. An administrator is troubleshooting a time synchronization problem for the router time to another Cisco IOS XE-based device that has recently undergone hardening.

Which action resolves the issue?

```
CPE# show ntp associations

 address         ref clock     st   when poll reach  delay
offset  disp
 ~10.1.255.40    .INIT.        16    -    64    0    0.000
0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker,
~ configured

CPE# debug ip icmp
*Feb 20 22:49:32.913: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
*Feb 20 22:50:37.918: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
*Feb 20 22:51:44.951: ICMP: dst (10.0.12.1) port unreachable rcv
from 10.1.255.40
```

**A.** Allow NTP in the ingress ACL on 10.1.255.40 by permitting TCP destined to port 123.
**B.** NTP service is disabled and must be enabled on 10.1.225.40.
**C.** Allow NTP in the ingress ACL on 10.1.225.40 by permitting UDP destined to port 123.
**D.** Ensure that he CPE router has a valid route to 10.1.255. 40 for NTP and rectify if not reachable.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 363**
Refer to the exhibit. The connected routers do not show up as OSPF neighbors. Which action resolves the issue?

```
R2# show ip ospf neighbor
R2#
R2# debug ip ospf hello

*Feb 22 23:46:58.699: OSPF-1 HELLO Et1/1: Rcv hello from
10.255.255.1 area 0 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Mismatched hello
parameters from 10.0.23.1
*Feb 22 23:46:58.703: OSPF-1 HELLO Et1/1: Dead R 30 C 20, Hello
R 10 C 10 Mask R 255.255.255.0 C 255.255.255.0
```

**A.** Change the R1 hello timer to 20.
**B.** Change the R2 dead timer to 20.
**C.** Change the R1 dead timer to 20.
**D.** Change the R2 hello timer to 20.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 364**
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?

```
router bgp 100
!
 neighbor 10.222.1.1 route-map SET-WEIGHT in
 neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map SET-WEIGHT permit 10
 match as-path 200
 set local-preference 250
 set weight 200
```

**A.** The local preference value in another neighbor statement is higher than 250.
**B.** The local preference value should be set to the same value as the weight in the route map.
**C.** The route map is applied in the wrong direction.
**D.** The weight value in another statement is higher than 200.
**Answer: D (LEAVE A REPLY)**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3se/3850/irg-xe-3se-3850-book/irg-prefix-filter.html

**NEW QUESTION: 365**
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 eq telnet
!
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
!
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)**

When assigning an IPv4 access list to an interface you used the ip access-list ACL_NAME in|out command in interface configuration mode. To assign an IPv6 ACL to an interface you'll use the ipv6 traffic-filter ACL_NAME in|out command in interface configuration mode.

We should also specific which port (telnet in this case) we want to deny or we will drop all TCP traffic to the destination.

Note: In fact there is an error with all of the above commands as we cannot use subnet mask (/64) with keyword "host". We must remove the subnet mask before applying the ACL statement.

**NEW QUESTION: 366**

How are LDP neighbors discovered?

**A.** Multicast hellos are sent to the 224.0.0.2 group address.

**B.** Unicast hellos are sent to directly connected neighbors IP addresses.

**C.** Multicast hellos are sent to the 224.0.0.5 group address.

**D.** Broadcasts hellos are sent to the 255.255.255.255 broadcast address.

**Answer: (SHOW ANSWER)**

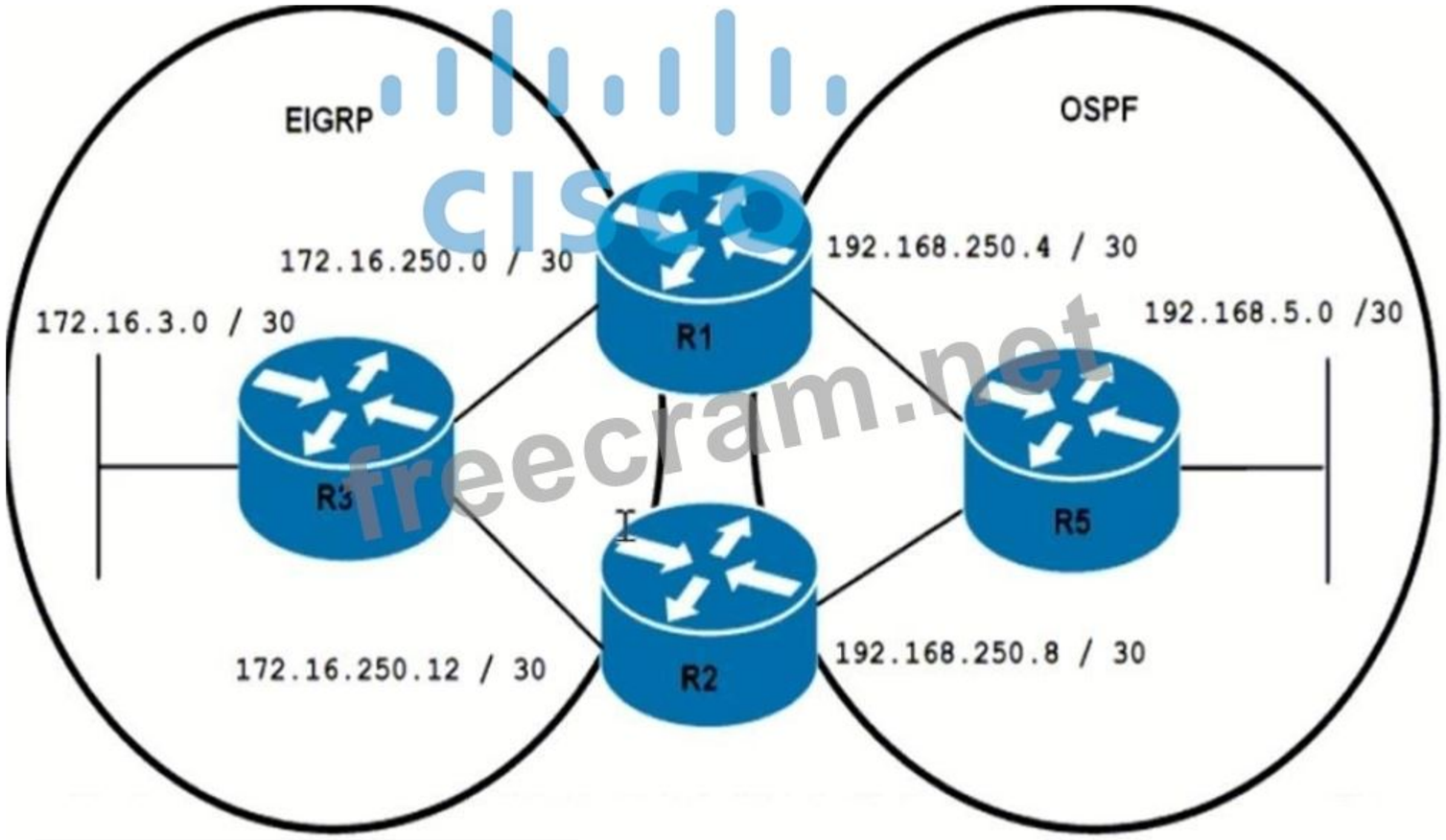
**NEW QUESTION: 367**

Refer to the exhibit. An engineer is troubleshooting a routing loop on the network to reach the 172.16 3.0/16 from the OSPF domain. Which configuration on router R1 resolves the issue?

```
R1#show running-config | begin router eigrp
router eigrp 100
 network 172.16.250.0 0.0.0.255
 redistribute ospf 1 metric 1 1 1 1 1
!
router ospf 1
 redistribute eigrp 100 subnets
 network 192.168.250.0 0.0.0.255 area 0
```

```
R2#show runn | begin router eigrp
router eigrp 100
 network 172.16.250.0 0.0.0.255
 redistribute ospf 1 metric 1 1 1 1 1
!
router ospf 1
 redistribute eigrp 100 subnets
 network 192.168.250.0 0.0.0.255 area 0
!
ip forward-protocol nd
```

```
R5#traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.250.9 66 msec
    192.168.250.6 6 msec
    192.168.250.9 8 msec
  2 172.16.250.2 33 msec
    172.16.250.14 88 msec
    172.16.250.2 11 msec
R5#
```




A.

```
router ospf 1
 redistribute eigrp 100 subnets route-map LOOPFILT
!
route-map LOOPFILT deny 10
 match ip address 15
!
route-map LOOPFILT permit 20
!
access-list 15 permit 172.16.0.0 0.0.255.255
```

B.

```
router eigrp 100
 redistribute ospf 1 metric 1 1 1 1 1 route-map LOOPFILT
!
route-map LOOPFILT deny 10
 match ip address 15
!
route-map LOOPFILT permit 20
!
access-list 15 permit 172.16.0.0 0.0.255.255
```

C.



D.



**Answer: (SHOW ANSWER)**

**NEW QUESTION: 368**

Refer to the exhibit. An engineer must troubleshoot an issue with the aaa authentication that affected the user's login to router R1. Which command allows the configured user to authenticate?

```
*Mar 10 20:13:58.156: AAA/BIND(00000055): Bind i/f
*Mar 10 20:13:58.156: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Mar 10 20:13:58.156: TAC+: Queuing AAA Authentication request 85 for processing
*Mar 10 20:13:58.156: TAC+:(00000055) login timer started 1020 sec timeout
*Mar 10 20:13:58.156: TAC+: processing authentication start request id 85
*Mar 10 20:13:58.156: TAC+: Authentication start packet created for 85()
*Mar 10 20:13:58.156: TAC+: Using server 10.106.60.182
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT: socket event 2
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: Would block while reading
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: read entire 18 bytes response
*Mar 10 20:13:58.156: TAC+:(00000055)/0/225FE2DC: Processing the reply packet
*Mar 10 20:13:58.156: TAC+:: received bad AUTHEN packet: length = 6, expected 43974
*Mar 10 20:13:58.156: TAC+:: Invalid AUTHEN packet (check keys).
```

**A.** aaa authentication login default group radius local
**B.** aaa authentication login default group radius tacacs+
**C.** aaa authentication login default group tacacs+
**D.** aaa authentication login default group radius

**Answer: (SHOW ANSWER)**

The debug log shows an "Invalid AUTHEN packet (check keys)" error, which indicates a mismatch between the shared key configured on the router and the TACACS+ server. Once the shared key is corrected on both the TACACS+ server and the router, the appropriate AAA authentication method must be applied.

The correct command is aaa authentication login default group tacacs+, which specifies that the router should use TACACS+ for authentication. If TACACS+ is the intended authentication method and the shared key is properly configured, this command ensures that the user can successfully log in to the router using TACACS+.

**NEW QUESTION: 369**

Which is statement about IPv6 inspection is true?

**A.** It learns and secures bindings for stateless autoconfiguration addresses in Layer 3 neighbor tables.
**B.** It learns and secures bindings for 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 Neighbor Discovery (ND) inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6- nd-inspect.html

**NEW QUESTION: 370**
Refer to the exhibit. Why is user authentication being rejected?

```
TAC+: TCP/IP open to 171.68.118.101/49 failed --
Destination unreachable; gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (2546660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure
```



**A.** The TACACS+ server expects "user" but the NT client sends "domain\user"
**B.** The TACACS+ server refuses the user because the user is set up for CHAP
**C.** The TACACS+ server is down and the user is in the local database
**D.** The TACACS+ server is down and the user is not in the local database
**Answer: (SHOW ANSWER)**
In the output we noticed that the "Destination unreachable; gateway or host down" notification while trying to communicate with the TACACS+ server. This means the TACACS+ server went down. So the next authentication method is via the local database ("Method=LOCAL"). But the authentication was failed again because of bad username, bad password or both.
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller- access-control-system-tacacs-/13864-tacacs-pppdebug.html

**NEW QUESTION: 371**
What are two features of BFD? (Choose two.)
**A.** replaces hello messages
**B.** reliable
**C.** scalable
**D.** intensive on CPU for Layer 2 links
**E.** requires routing protocols
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 372**
Refer to the exhibit. An administrator configured a Cisco router for TACACS authentication, but the router is using the local enable password instead. Which action resolves the issue?

**Configuration Output:**

```
aaa new-model
aaa group server tacacs+ admin
server name admin
!
ip tacacs source-interface GigabitEthernet1
aaa authentication login admin group tacacs+ local enable
aaa session-id common
!
tacacs server admin
address ip 10.11.15.6
key 7 01150F165E1C07032D
!
line vty 0 4
login authentication admin
```

**Debug Output:**

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



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

**NEW QUESTION: 373**
What is a prerequisite for configuring BFD?
**A.** All routers in the path between two BFD endpoints must have BFD enabled.
**B.** Jumbo frame support must be configured on the router that is using BFD.
**C.** Cisco Express Forwarding must be enabled on all participating BFD endpoints.
**D.** To use BFD with BGP. the timers 3 9 command must first be configured in the BGP routing process.
**Answer: (SHOW ANSWER)**
https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html#wp1043332

**NEW QUESTION: 374**
What are two purposes of using IPv4 and VPNv4 address-family configurations in a Layer 3 MPLS VPN? (Choose two.)
**A.** RD is prepended to the IPv4 route to make it unique.
**B.** The VPNv4 address consists of a 64-bit route distinguisher that is prepended to the IPv4 prefix.

**C.** MP-BGP is used to allow overlapping IPv4 addresses between customers to advertise through the network.
**D.** The IPv4 address is needed to tag the MPLS label.
**E.** The VPNv4 address is used to advertise the MPLS VPN label.
**Answer: (SHOW ANSWER)**
VPNv4 address consists of 64-bit Route Distinguisher (RD) prepended to IPv4 prefix. This is to make routes unique that are in different VRFs.

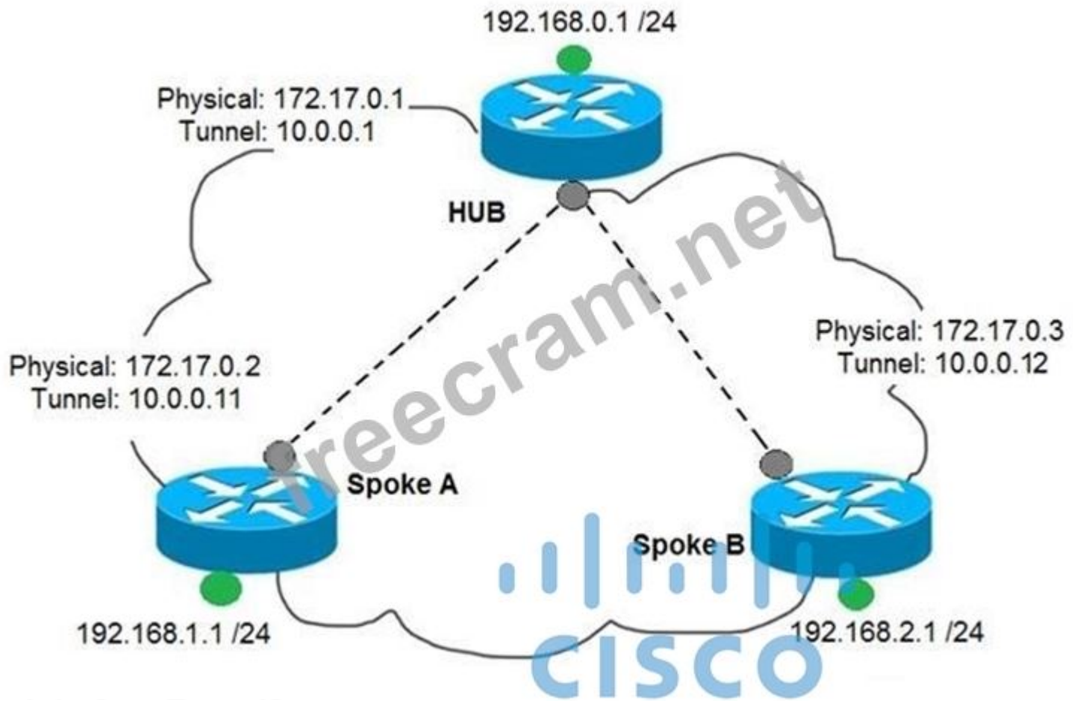
**NEW QUESTION: 375**
Refer to the exhibit. An engineer wanted to set a tag of 30 to route 10.1.80.65/32 but it failed.
How is the issue fixed?

```
R1

ip prefix-list ccnp1 seq 5 permit 10.1.48.0/24 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.0/24 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.0/24 le 24

route-map ospf-to-eigrp permit 10
   match ip address prefix-list ccnp1
   set tag 30
route-map ospf-to-eigrp permit 20
   match ip address prefix-list ccnp2
   set tag 20
route-map ospf-to-eigrp permit 30
   match ip address prefix-list ccnp3
   set tag 10
```



**A.** Modify route-map ospf-to-eigrp permit 10 and match prefix-list ccnp2.
**B.** Modify route-map ospf-to-eigrp permit 30 and match prefix-list ccnp2.
**C.** Modify prefix-list ccnp3 to add 10.1.64.0/20 le 24.
**D.** Modify prefix-list ccnp3 to add 10.1.64.0/20 ge 32.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 376**
Refer to the exhibit. Which interface configuration must be configured on the spoke A router to enable a dynamic DMVPN tunnel with the spoke B router?




A.
```
interface Tunnel0
description mGRE – DMVPN Tunnel
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel destination FastEthernet 0/0
tunnel mode gre multipoint
```

B.
```
interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source FastEthernet 0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
ip nhrp map 10.0.0.1 172.17.0.1
```

C.
```
interface Tunnel0
ip address 10.1.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source 1.1.1.10
ip nhrp map 10.0.0.11 172.17.0.2
tunnel mode gre
```
D.
```
interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast static
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint
```

**Answer: (SHOW ANSWER)**

The command "ip nhrp map multicast dynamic" should be only used on Hub router, not spoke. If we are running dynamic routing protocols based on multicast (like RIP, OSPF, EIGRP ...) we have to add the command "ip nhrp map multicast dynamic" in Hub to replicate all multicast traffic to all dynamic entries in the NHRP table (multicast will be proceeded as unicast traffic) -> Answer A is not correct. Also another error in this answer is the "tunnel source" IP address. It should be the NBMA address of the Spoke interface: 172.17.0.2.

Answer C is not correct as the "tunnel source 1.1.1.10", "ip nhrp map 10.0.0.11 172.17.0.2" and

"tunnel mode gre" are wrong.

Answer D is not correct as there is no "ip nhrp map multicast static" command, only the "ip nhrp map multicast <static-IP>" command is available. The "tunnel source 10.0.0.1" is not correct either.

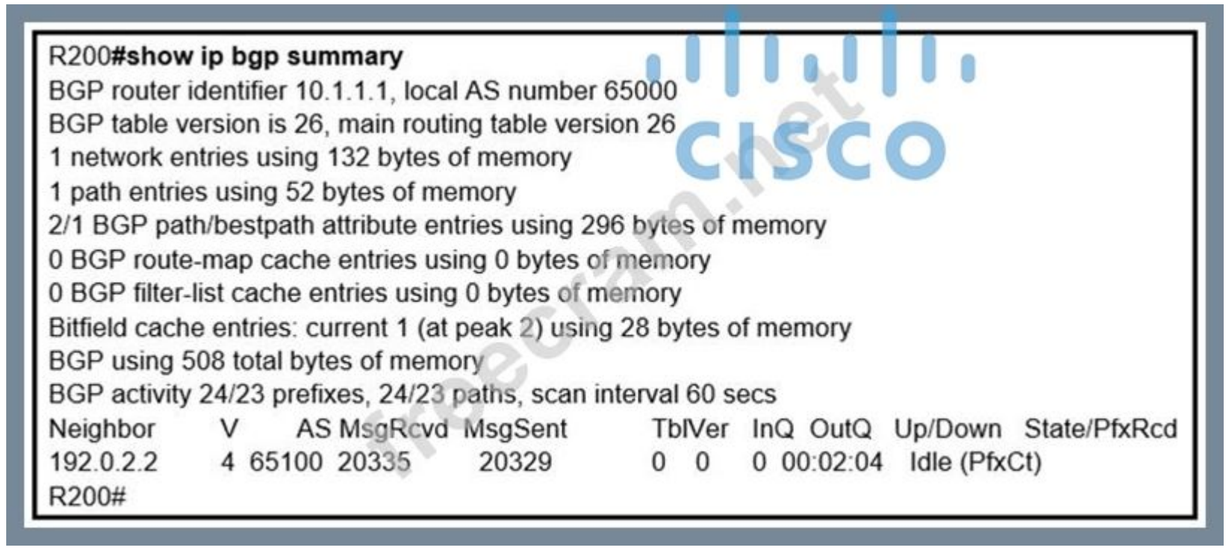
Answer B is correct. The " tunnel source FastEthernet0/0" is equivalent to "tunnel source

172.17.0.2", which is the NBMA address of Spoke A.



**NEW QUESTION: 377**

Refer to the exhibit. In which circumstance does the BGP neighbor remain in the idle condition?




**A.** if prefixes are not received from the BGP peer

**B.** if prefixes reach the maximum limit

**C.** if a prefix list is applied on the inbound direction

**D.** if prefixes exceed the maximum limit

**Answer: (SHOW ANSWER)**

The BGP Maximum-Prefix feature allows you to control how many prefixes can be received from a neighbor. By default, this feature allows a router to bring down a peer when the number of received prefixes from that peer exceeds the configured Maximum-Prefix limit.

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/25160-bgp- maximum- prefix.html#:~:text=The%20BGP%20Maximum%2DPrefix%20feature%20allows%20you%20to%20control%20how,the%20configured%20Maximum%2DPrefix%20limit.