Cisco Certified Network Professional Enterprise (CCNP 2025)

Exam 300-410 Enterprise Advanced Routing and Services (ENARSI)

Demo Questions

CISCO

CISCO CERTIFIED CCNP

300-410: Cisco Enterprise Advanced Routing and Services

注意：題目有 ⭐ 標記只代表近期出過的題目，⭐ 數量越多，代表過去一個月出的次數越多，但同學必須溫習“整份”題目才可提升考試合格機會。

QUESTION 1

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

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

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

Refer to the exhibit. An administrator must harden a router, but the administrator failed to test the SSH access successfully to the router. Which action resolves the issue?

A. SSH must be allowed with the **`transport output ssh`** command
B. Configure **`enable secret`** to log in to the device
C. Configure SSH on the remote device to log in using SSH
D. SSH syntax must be **`ssh -l user ip`** to log in to the remote device

Answer: D

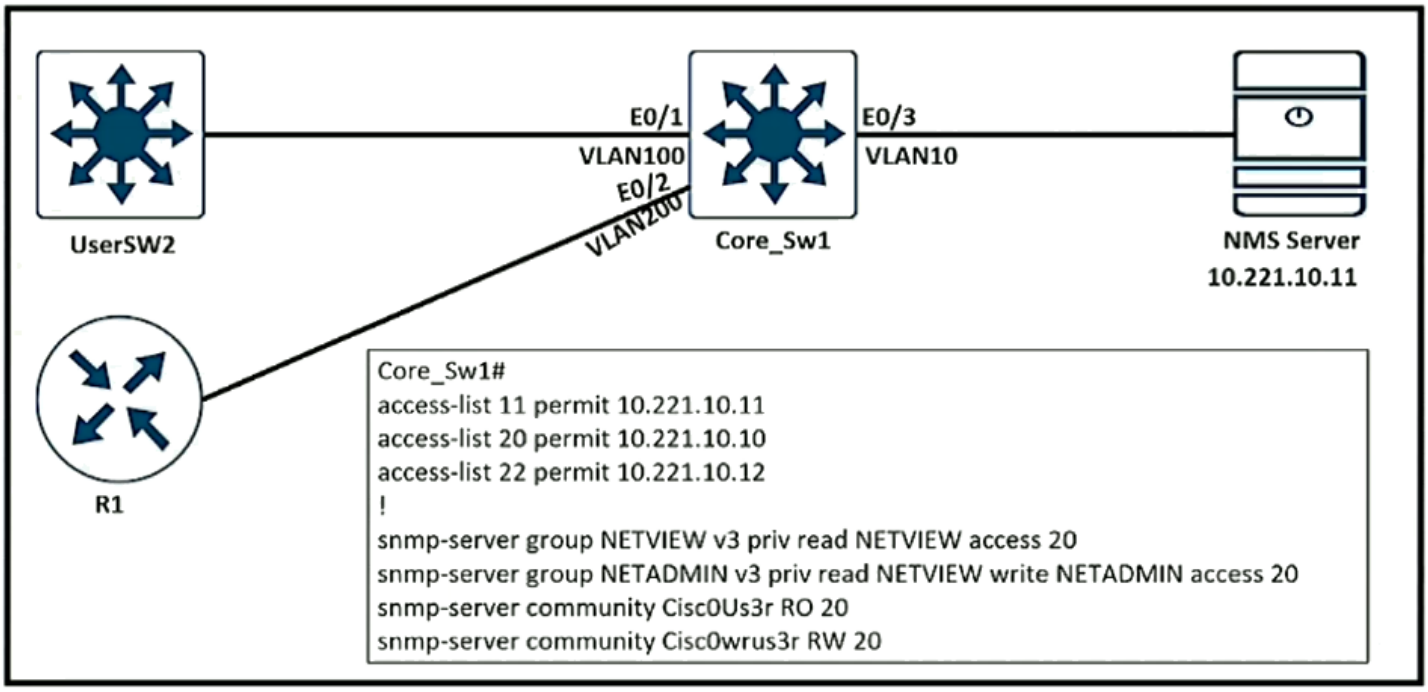
QUESTION 2

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

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

Answer: C, E

QUESTION 3



Refer to the exhibit. An engineer configured SNMP communities on the Core_Sw1, but the SNMP server cannot obtain information from Core_Sw1. Which configuration resolves this issue?

A. `snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22`

B. `snmp-server group NETVIEW v2c priv read NETVIEW access 22`

C. `access-list 20 permit 10.221.10.11`

D. `access-list 20 permit 10.221.10.12`

Answer: C

QUESTION 4

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 2 name ISP2
```

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

A. Include a valid source-interface keyword in the icmp-echo statement

B. Modify the threshold to match the administrative distance of the ISP2 route

C. Modify the static routes to refer both to the next hop and the outgoing interface

D. Reference the track object 1 on the default route through ISP2 instead of ISP1

Answer: B

QUESTION 5

An engineer configured a company's multiple area OSPF Head Office router and SiteA Cisco routers with VRF lite. Each site router is connected to a PE router of an MPLS backbone:

Head Office & Site A

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

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

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

Answer: B

QUESTION 6

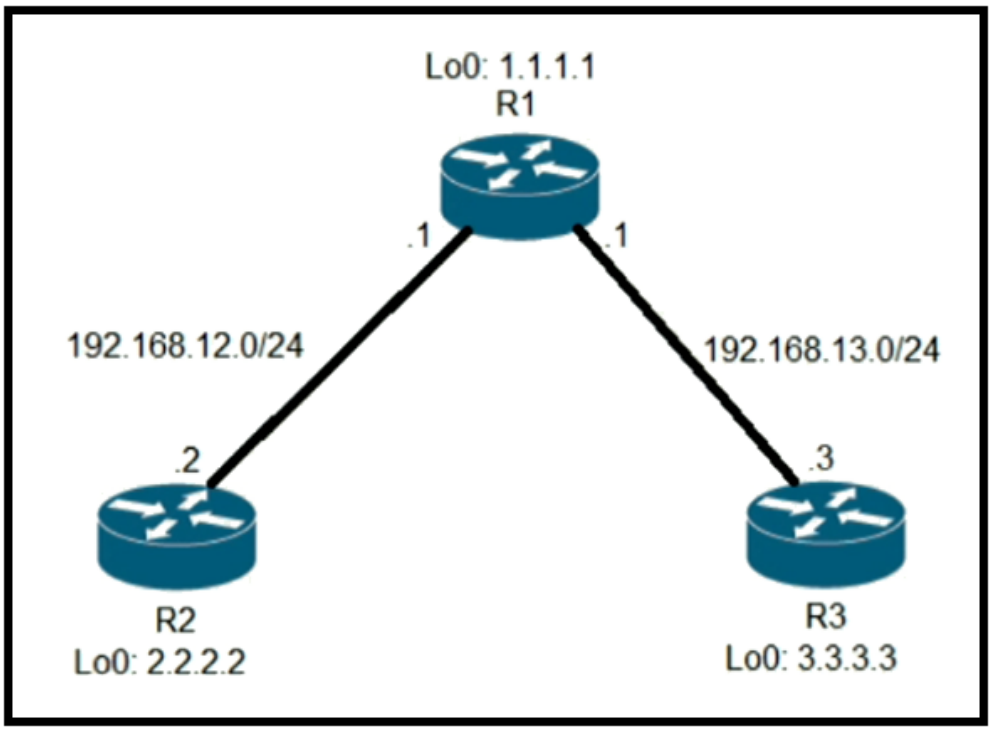
```
*Jun 24 08:54:51.530: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:52.525: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jun 24 08:54:52.528: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition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

Refer to the exhibit. R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1. What action will fix the issue?

A. Fix route dampening configured on the router.
B. Fix IP Event Dampending configured on the interface.
C. Correct the IP SLA probe that failed.
D. Replace the SFP module because it is not support.

Answer: B

QUESTION 7



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

A. Use a leak map on R1 that matches the required prefix and apply it with the distribute list command toward R3.
B. Use a leak map on R4 that matches the required prefix and apply it with the EIGRP stub feature.
C. Add a static null route for R2 loopback address in R1 and redistribute it to advertise to R3.
D. Add a static route for R2 loopback address in R1 and redistribute it to advertise to R3.

Answer: A

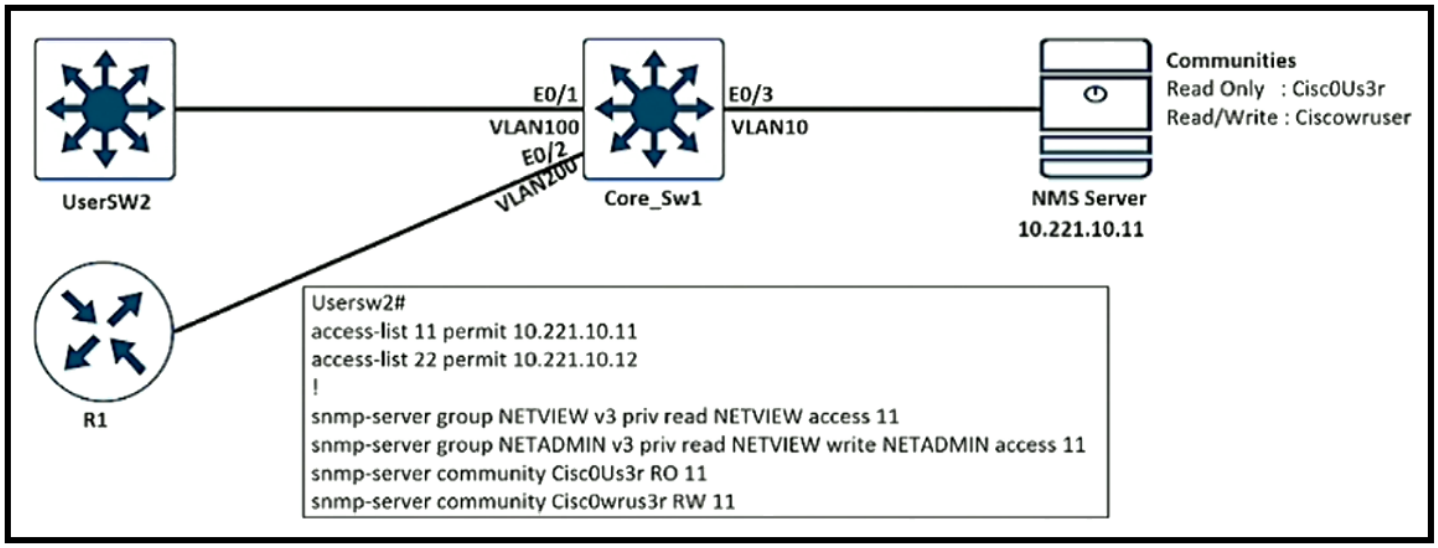
QUESTION 8

An engineer configured routing between multiple OSPF domains and introduced a routing loop that caused network instability. Which action resolves the problem?

A. Set a tag using the **redistribute** command toward a domain and deny inbound in the other domain by a matching tag
B. Set a tag using the **redistribute** command toward a different domain and deny the matching tag when exiting from that domain
C. Set a tag using the **network** command in a domain and use the **route-map** command to deny the matching tag when exiting toward a different domain
D. Set a tag using the **network** command in a domain and use the **route-map** command to deny the matching tag when entering into a different domain

Answer: B

QUESTION 9



Refer to the exhibit. An engineer configured SNMP Communities on UseSW2 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 group NETADMIN v3 priv read NETVIEW write NETADMIN access 22`**

C. **`snmp-server community Ciscowruser RW 11`**

D. **`snmp-server community Cisc0Us3r1 RW 11`**

Answer: A

QUESTION 10

```
%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
```

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

A. Configure the debug uptime option

B. Configure the msec option

C. Configure the timezone option

D. Configure the log uptime option

Answer: B

QUESTION 11

```
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
```

Refer to the exhibit. A client is concerned that passwords are visible when running this **show archive log config all**. Which router configuration is needed to resolve this issue?

A. MASS-RTR(config)# **service password-encryption**
B. MASS-RTR(config)# **aaa authentication arap**
C. MASS-RTR(config-archive-log-cfg)# **hidekeys**
D. MASS-RTR(config-archive-log-cfg)# **password encryption aes**

Answer: C

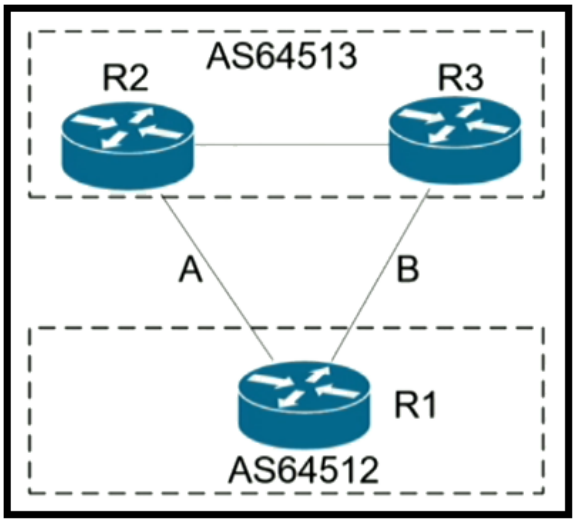
QUESTION 12

What is the purpose of an OSPF sham-link?

A. to allow inter-area routing when OSPF is used as the PE-CE connection protocol in an MPLS VPN network
B. to allow intra-area routing when OSPF is used as the PE-CE connection protocol in an MPLS VPN network
C. to connect OSPF backdoor routing when OSPF is used as the PE-PE connection protocol in an MPLS VPN network
D. to connect OSPF backdoor routing when OSPF is used as the PE-CE connection protocol in an MPLS VPN network

Answer: C

QUESTION 13



Refer to the exhibit. A network engineer for AS64512 must6 remove the inbound and outbound traffic from link A during maintenance without closing the BGP session so that there is still a backup link over link A toward the ASN. Which BGP configuration on R1 accomplishes this goal?

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

B.
```
route-map link-a-in permit 10
 set local-preference 200
route-map link-a-out permit 10
route-map link-b-in permit 10
route-map link-b-out permit 10
 set as-path prepend 64512
```

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

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

Answer: C

QUESTION 14

Debug output:

```
May 5 15:19:26.173: OSPF: Send DBD to 192.168.95.11 on GigabitEthernet3/1 seq 0x2AC opt 0x50 flag 0x7 len 32
May 5 15:19:30.749: OSPF: Send DBD to 192.168.95.11 on GigabitEthernet3/1 seq 0x2AC opt 0x50 flag 0x7 len 32
May 5 15:19:30.749: OSPF: Retransmitting DBD to 192.168.95.11 on GigabitEthernet3/1 [1]
May 5 15:19:35.509: OSPF: Send DBD to 192.168.95.11 on GigabitEthernet3/1 seq 0x2AC opt 0x50 flag 0x7 len 32
May 5 15:27:29.904: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.22 on Tunnel0 from LOADING to FULL, Loading Done
May 5 15:28:28.176: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.22 on Tunnel9 from LOADING to FULL, Loading Done
May 5 15:30:02.028: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.22 on Tunnel55 from LOADING to FULL, Loading Done
May 5 15:30:34.720: %CRYPTO-4-IKE_DEFAULT_POLICY_ACCEPTED: IKE default policy was matched and is being used.
May 5 15:30:44.009: %CRYPTO-4-IKE_DEFAULT_POLICY_ACCEPTED: IKE default policy was matched and is being used.
May 5 15:19:30.749: OSPF: Send DBD to 192.168.95.11 on GigabitEthernet3/1 seq 0x2AC opt 0x50 flag 0x7 len 32
May 5 15:19:30.749: OSPF: Retransmitting DBD to 192.168.95.11 on GigabitEthernet3/1 [1]
May 5 15:31:09.441: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.22 on Tunnel9 from LOADING to FULL, Loading Done
May 5 15:31:27.341: %CRYPTO-4-IKE_DEFAULT_POLICY_ACCEPTED: IKE default policy was matched and is being used.
May 5 15:31:42.137: %CRYPTO-4-IKE_DEFAULT_POLICY_ACCEPTED: IKE default policy was matched and is being used.
May 5 15:32:14.777: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.22 on Tunnel55 from LOADING to FULL, Loading Done
May 5 15:19:30.749: OSPF: Send DBD to 192.168.95.11 on GigabitEthernet3/1 seq 0x2AC opt 0x50 flag 0x7 len 32
May 5 15:19:30.749: OSPF: Retransmitting DBD to 192.168.95.11 on GigabitEthernet3/1 [1]
May 5 15:33:40.761: %CRYPTO-4-IKE_DEFAULT_POLICY_ACCEPTED: IKE default policy was matched and is being used.
May 5 15:34:32.065: %CRYPTO-4-IKE_DEFAULT_POLICY_ACCEPTED: IKE default policy was matched and is being used.
May 5 15:35:05.950: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.22 on Tunnel0 from LOADING to FULL, Loading Done
May 5 15:56:36.603: %PARSER-5-CFGLOG_LOGGEDCMD: User:gua logged command:!exec: enable
```

Refer to the exhibit. A network administrator is troubleshooting OSPF adjacency issue by going through the console logs in the router, but due to an overwhelming log messages stream, it is impossible to capture the problem. Which two commands reduce console log messages to relevant OSPF neighbor problem details so that the issue can be resolved? (Choose two)

A. **`debug condition all`**
B. **`debug condition interface`**
C. **`debug condition session-id ADJCHG`**
D. **`debug condition ospf neighbor`**
E. **`debug condition ip`**

Answer: B, C

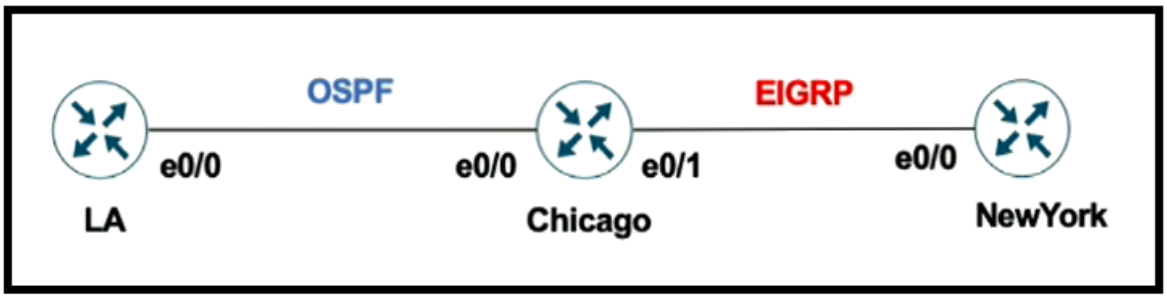
QUESTION 15 

Which component of MPLS VPNs is used to extend the IP address so that an engineer is able to identify to which VPN it belongs?

A. VPNv4 address family
B. RD
C. LDP
D. RT

Answer: B

QUESTION 16



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 the NewYork router does not receive any LA routes. Which configuration fixes the problem on the Chicago router?

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

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

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

D.
```
router ospf 1
   redistribute eigrp 100 metric 20
```

Answer: C

QUESTION 17

Which failure detection mechanism is used for BFD?

A. variable rate
B. consistent rate
C. Layer 2 protocol failure
D. routing protocol failure

Answer: B

https://www.cisco.com/en/US/technologies/tk648/tk365/tk381/technologies_white_paper0900aecd80243ff4.html

QUESTION 18

```
Switch(config)# ip vrf 70
Switch(config-vrf)# rd 70:1
Switch(config-vrf)# route-target export 70:1
Switch(config-vrf)# route-target import 70:1
Switch(config-vrf)# exit
Switch(config)# ip vrf 80
Switch(config-vrf)# rd 80:1
Switch(config-vrf)# route-target export 80:1
Switch(config-vrf)# route-target import 80:1
```

Refer to the exhibit. An engineer must extend VRF-Lite over a trunk to another switch for VLAN 70 (10.70.70.0/24) on port GigabitEthernet0/0 and VLAN 80 (10.80.80.0/24) on port GigabitEthernet0/1. Which configuration accomplishes this objective?

A.
```
interface GigabitEthernet0/0
switchport mode access
switchport access vlan 70
!
interface GigabitEthernet0/1
switchport mode access
switchport access vlan 80
```

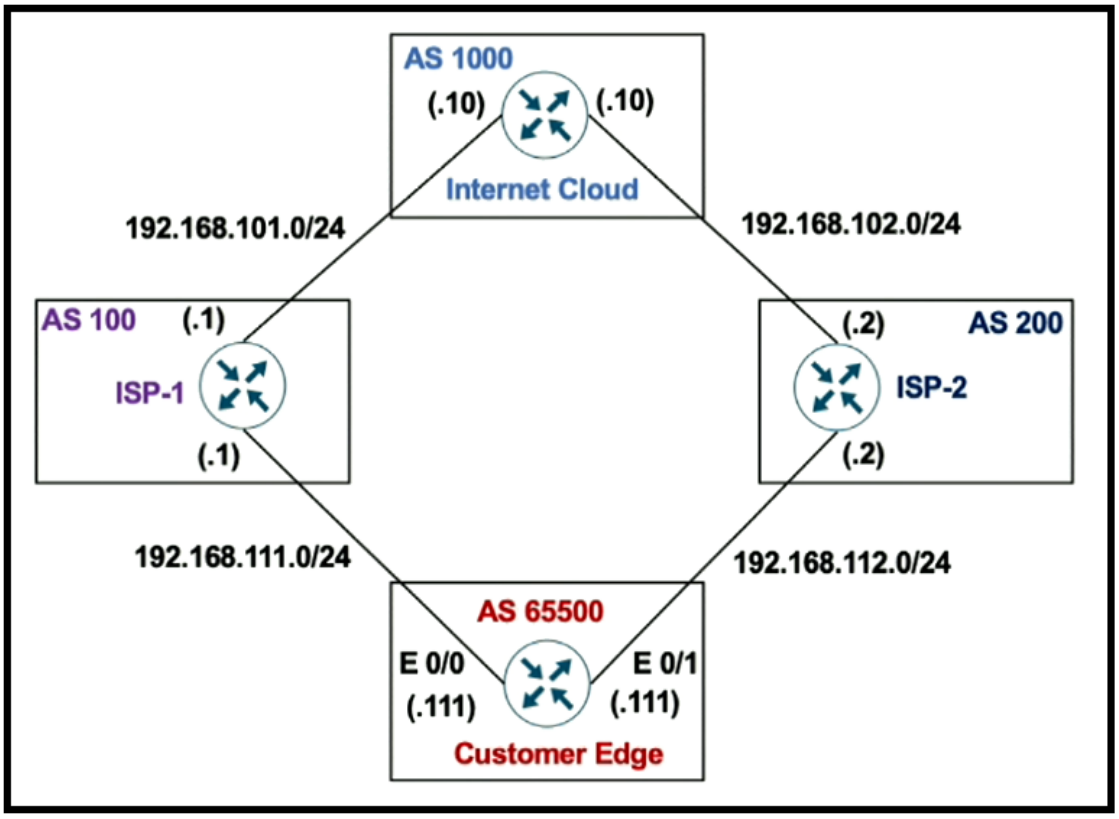
B.
```
interface GigabitEthernet0/0
no switchport
ip vrf forwarding 70
ip address 10.70.70.1 255.255.255.0
!
interface GigabitEthernet0/1
no switchport
ip vrf forwarding 80
ip address 10.80.80.1 255.255.255.0
```

C.
```
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 70
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 80
```

D.
```
interface GigabitEthernet0/0
switchport mode access
switchport access vlan 70
ip vrf forwarding 70
!
interface GigabitEthernet0/1
switchport mode access
switchport access vlan 80
ip vrf forwarding 80
```

Answer: C

QUESTION 19



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

```
Customer-Edge
route-map SETLP
 set local-preference 111
!
router bgp 64550
 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 SETPP
 set as-path prepend 100 100
 !
 router bgp 65550
 neighbor 192.168.111.1 remote-as 100
 neighbor 192.168.111.1 route-map SETPP in
```

B.
```
route-map SETPP
 set as-path prepend 111 111
 !
 router bgp 65550
```

```
neighbor 192.168.111.1 remote-as 100
neighbor 192.168.111.1 route-map SETPP out
```

C.
```
route-map SETLP
set local-preference 111
!
router bgp 65550
neighbor 192.168.111.1 remote-as 100
neighbor 192.168.111.1 route-map SETLP in
```

D.
```
route-map SETLP
set local-preference 111
!
router bgp 65550
neighbor 192.168.111.1 remote-as 100
neighbor 192.168.111.1 route-map SETLP out
```

Answer: C

QUESTION 20

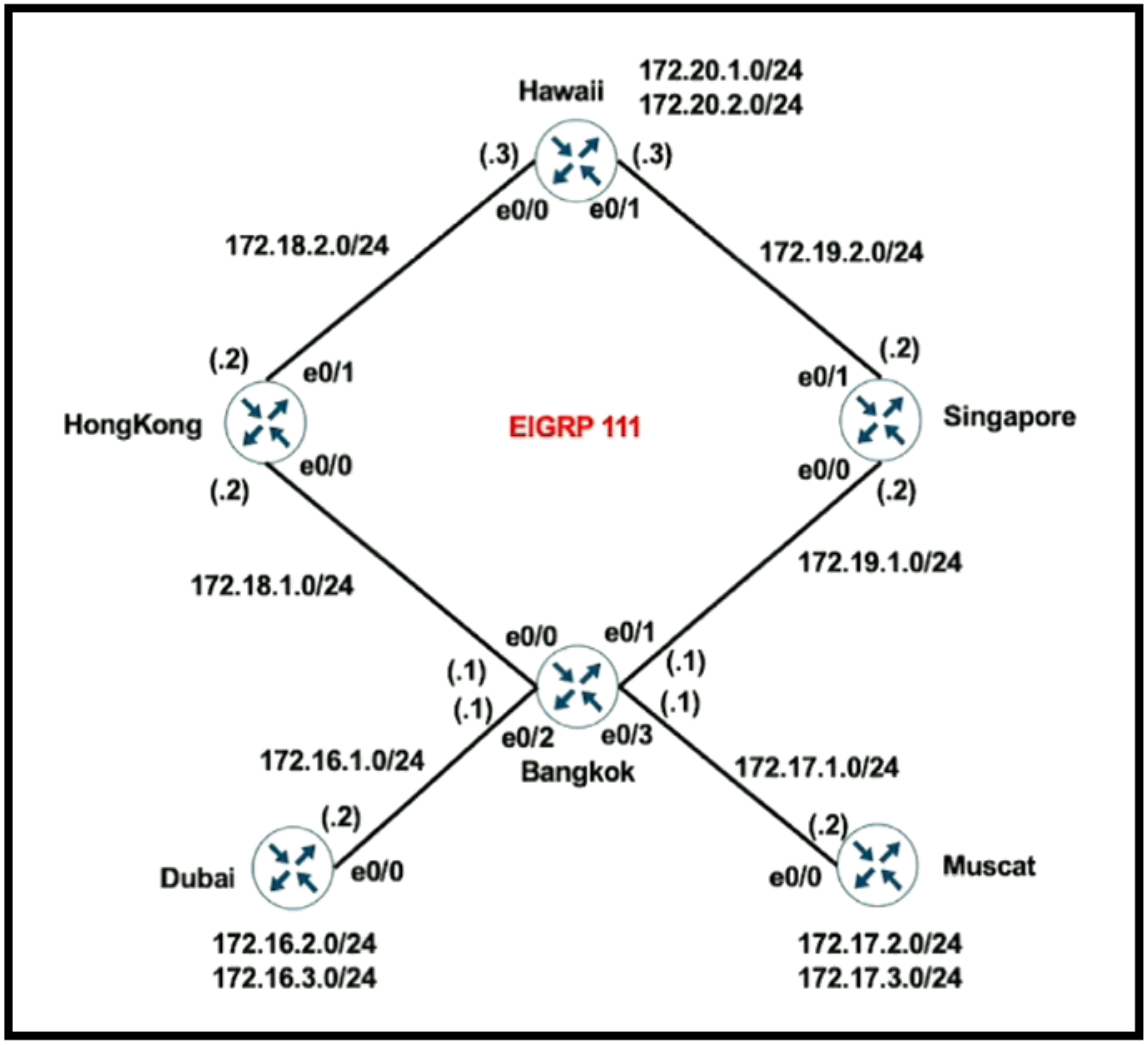
```
R1#show ip route ospf

     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
```

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?

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

Answer: B

QUESTION 21



Refer to the exhibit. Bangkok is using ICMP 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. **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
```

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 Ethernet0/2
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
!
interface Ethernet0/0
ip policy route-map PBR1
```

D. **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
```

Answer: B

QUESTION 22

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

A. **`ip nhrp map dynamic`**

B. **`ip nhrp nhs multicast`**

C. **`ip nhrp redirect`**

D. **`ip nhrp shoutcut`**

Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-summ-maps.html

QUESTION 23

Network operations report issues with receiving too many external routes, which caused CPU spike on routers with smaller memories. Which action resolves the issue?

A. Configure the **`area range`** command when redistributing on ABR

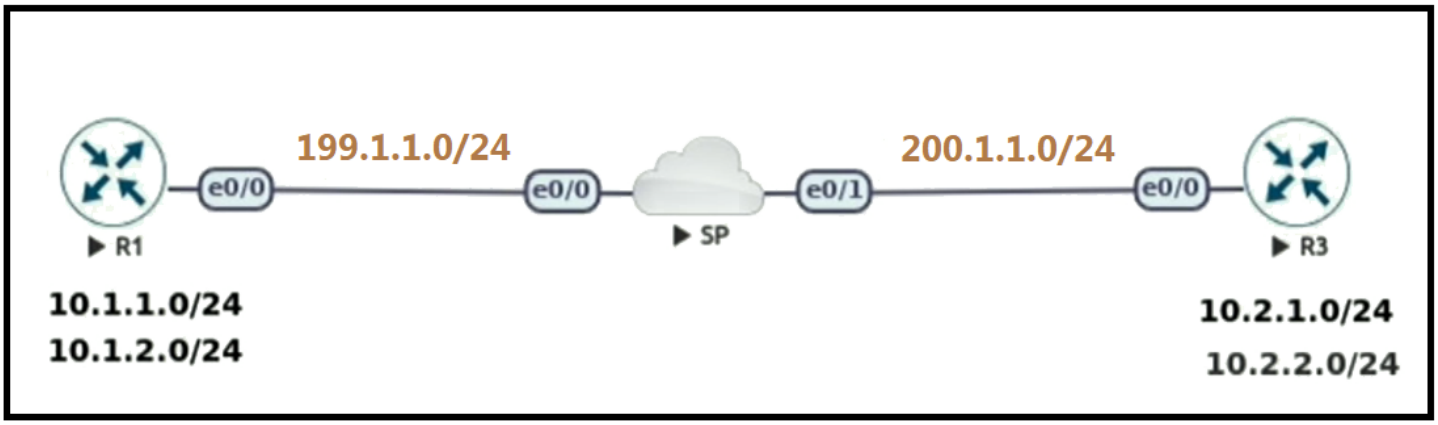
B. Configure the **`area range`** command when redistributing on ASBR

C. Configure the **`summary-address`** command when redistributing on ABR

D. Configure the **`summary-address`** command when redistributing on ASBR

Answer: D

QUESTION 24



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

A.
```
crypto isakp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
crypto isakmp key cisco123 address 199.1.1.1
```

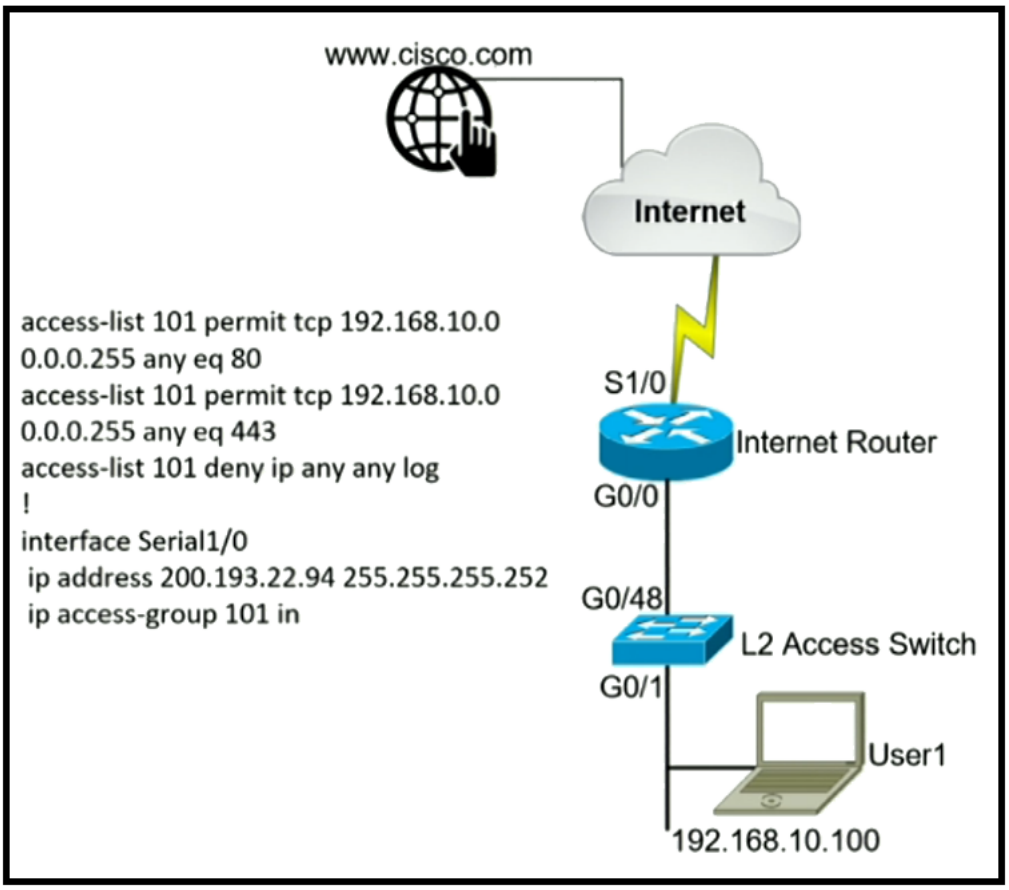
B.
```
crypto isakp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
crypto isakmp key cisco123 address 200.1.1.3
```

C.
```
crypto isakp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
crypto isakmp key cisco123! address 199.1.1.1
```

D.
```
crypto isakp policy 5
authentication pre-share
encryption 3des
hash sha
group 2
!
crypto isakmp key cisco123 address 200.1.1.3
```

Answer: D

QUESTION 25



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

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

Answer: B

QUESTION 26

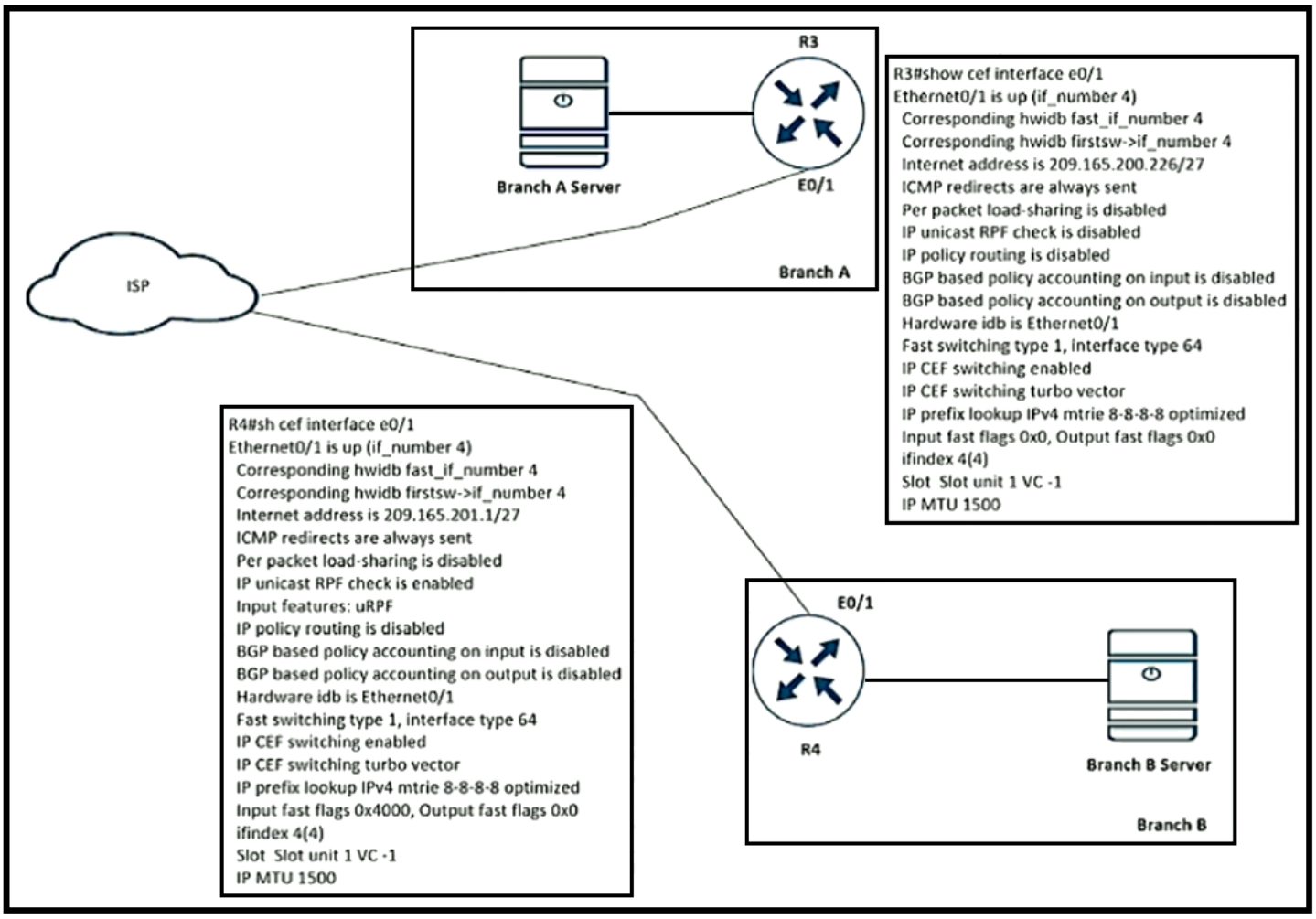
A network administrator performed a Compact Flash Memory upgrade on a Cisco Catalyst 6509 Switch. Everything is functioning normally except SNMP, which was configured to monitor the bandwidth of key interfaces but the interface indexes are changed. Which global configuration resolves the issue?

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

Answer: D

https://community.cisco.com/t5/network-management/snmp-errors/td-p/672696

QUESTION 27



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

A. **R3**

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

B. **R4**

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

C. **R3**

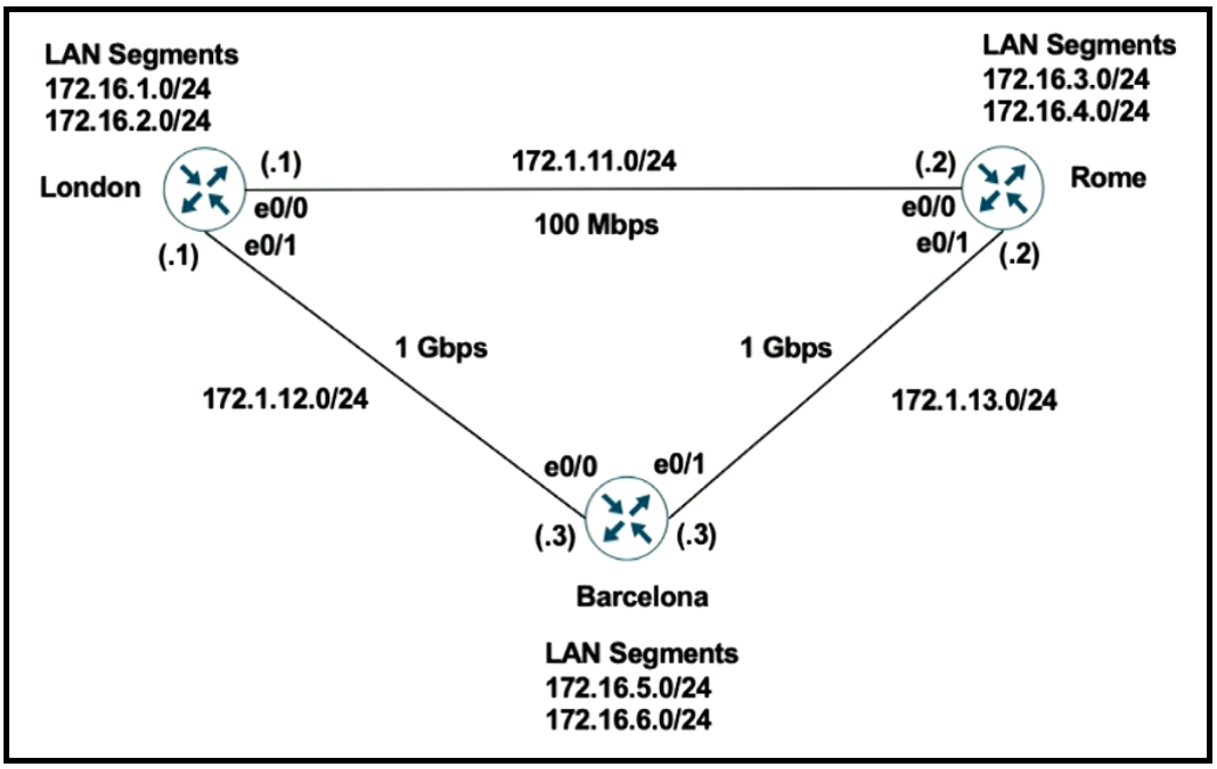
```
interface ethernet0/1
ip unicast RPF check reachable-via any allow-default allow-self-ping
```

D. **R4**

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

Answer: A

QUESTION 28



London – "show ip route" output

```
Gateway of last resort is not set

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

Rome - "show run | section router" output

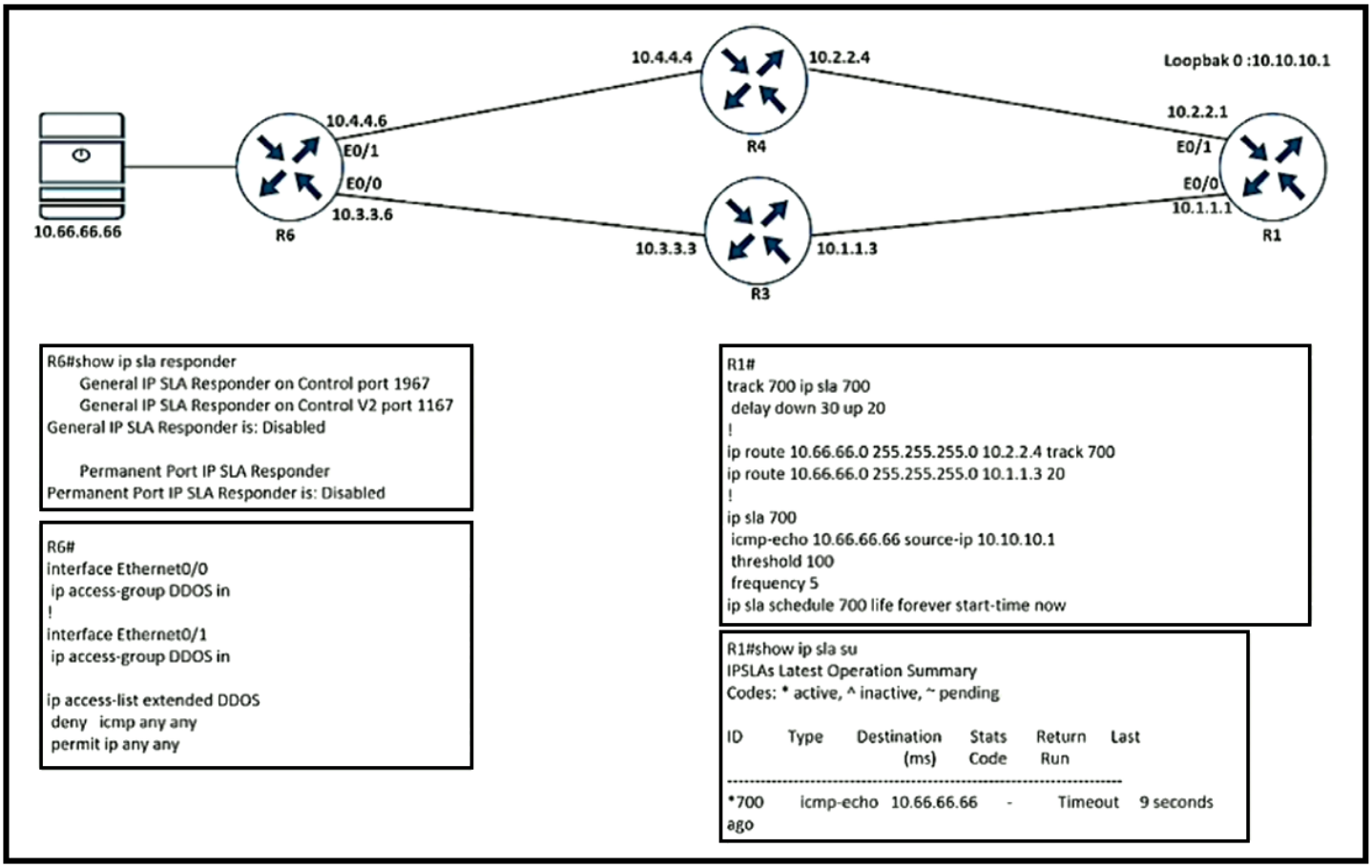
```
router eigrp 111
  network 172.1.0.0
  redistribute connected
!
router rip
  version 2
  network 172.1.0.0
  network 172.16.0.0
  no auto-summary
```

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

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

Answer: D

QUESTION 29



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

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

B. **R6(config)# ip sla responder udp-echo ip address 10.10.10.1 port 5000**

C. **R6(config)# ip access-list extended DDOS**
R6(config-ext-nacl)# 5 permit icmp host 10.10.10.1 host 10.66.66.66

D. **R6(config)# ip access-list extended DDOS**
R6(config-ext-nacl)# 5 permit icmp host 10.66.66.66 host 10.10.10.1

Answer: C

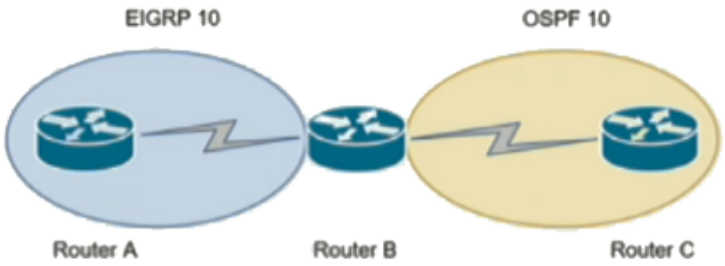
QUESTION 30

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

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

Answer: C

QUESTION 31




```
RouterB:

router eigrp CLASS
 !
 address-family ipv4 unicast autonomous-system 10
  !
  topology base
   redistribute ospf 10 match external 1 external 2 metric 1000000 10 255 1 1500
  exit-af-topology
  network 172.16.2.2 0.0.0.0
  eigrp router-id 2.2.2.2
 exit-address-family

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet0/0
L        172.16.1.2/32 is directly connected, GigabitEthernet0/0
C        172.16.2.0/30 is directly connected, GigabitEthernet0/1
L        172.16.2.2/32 is directly connected, GigabitEthernet0/1
      192.168.0.0/32 is subnetted, 1 subnets
O        192.168.0.1 [110/2] via 172.16.1.1, 1d03h, GigabitEthernet0/0
      192.168.1.0/32 is subnetted, 1 subnets
O        192.168.1.1 [110/2] via 172.16.1.1, 1d03h, GigabitEthernet0/0
      192.168.2.0/32 is subnetted, 1 subnets
O        192.168.2.1 [110/2] via 172.16.1.1, 1d03h, GigabitEthernet0/0
D     192.168.11.0/24 [90/10880] via 172.16.2.1, 1d03h, GigabitEthernet0/1
D     192.168.12.0/24 [90/10880] via 172.16.2.1, 1d03h, GigabitEthernet0/1
D     192.168.13.0/24 [90/10880] via 172.16.2.1, 1d03h, GigabitEthernet0/1
```

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

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

Answer: B

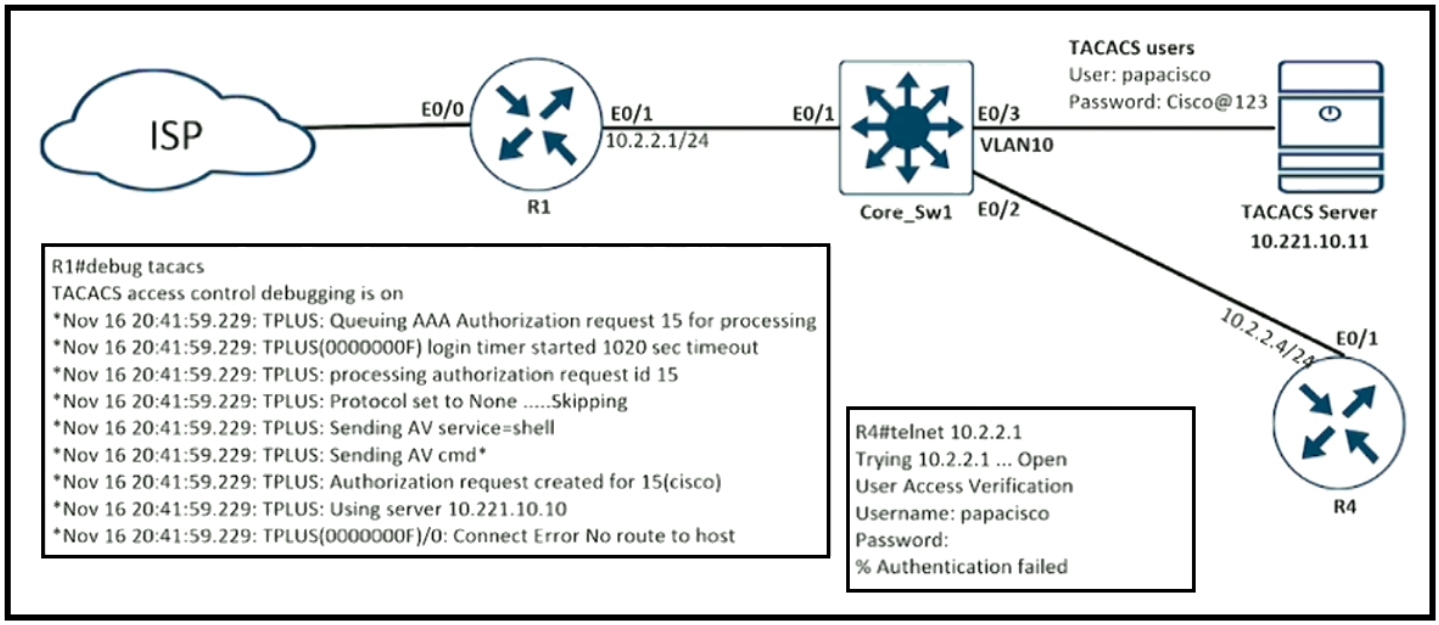
QUESTION 32

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

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

Answer: B

QUESTION 33



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

A. `ip route 10.221.0.11 255.255.255.255 ethernet 0/1`

B. `ip route 10.221.10.10 255.255.255.255 ethernet 0/1`

C.
```
tacacs server prod
address ipv4 10.221.10.10
exit
```

D.
```
tacacs server prod
address ipv4 10.221.10.11
exit
```

Answer: D

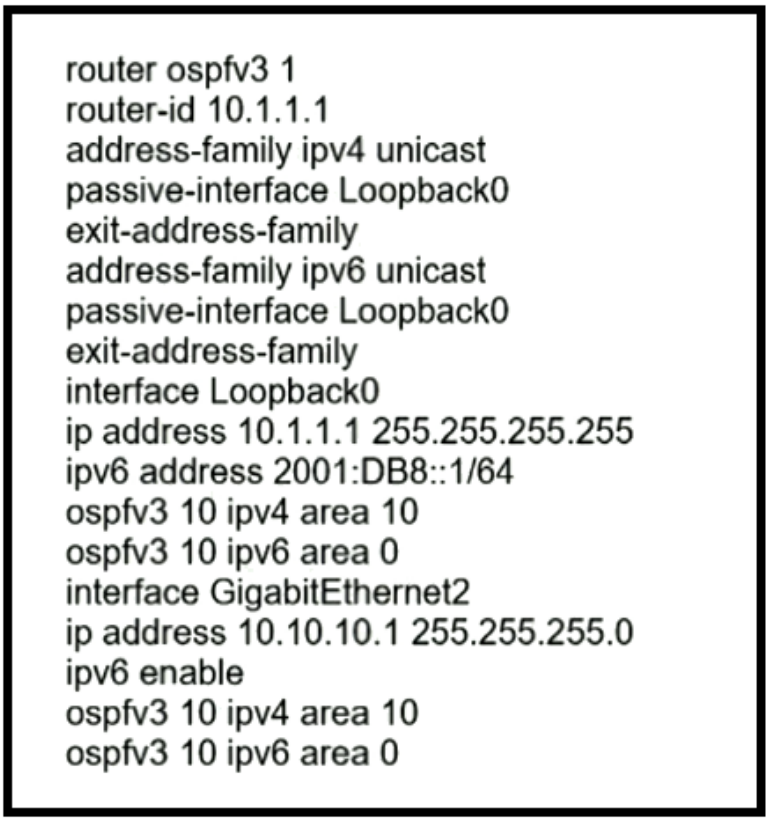
QUESTION 34

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

A. Enable service distribution from the Systems 360 page.
B. Click the master host node with all the services and select services to be moved to other hosts.
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: A

QUESTION 35



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?

A. Replace OSPF process 10 on the interfaces with OSPF process 1 for the IPv4 address, and remove process 10 from the global configuration
B. Replace OSPF process 10 on the interfaces with OSPF process 1 for the IPv6 address, and remove process 10 from the global configuration
C. Replace OSPF process 10 on the interfaces with OSPF process 1, and remove process 10 from the global configuration
D. Replace OSPF process 10 on the interfaces with OSPF process 1, and configure an additional router ID with IPv6 address

Answer: C

QUESTION 36

Which label operations are performed by a label edge router?

A. SWAP and PUSH
B. SWAP and POP
C. PUSH and POP
D. PUSH and PHP

Answer: C

QUESTION 37

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
!
policy-map PM-COPP
class CLASS-SSH
no police 500000 conform-action transmit
police 500000 conform-action transmit exceed-action drop
```

B.
```
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
```

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
!
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
```

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

Answer: B

QUESTION 38

```
R4#
interface FastEthernet1/0
 ip address 10.1.1.14 255.255.255.252
 ip access-group VENDOR in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 EIGRPKEY
 speed 100
 full-duplex
!
interface loopback 100
 ip address 10.199.100.1 255.255.255.255
!
router eigrp 100
 network 10.1.1.8 0.0.0.3
 network 10.1.1.12 0.0.0.3
 no auto-summary
 eigrp router-id 100.4.4.4
 neighbor 10.1.1.13 FastEthernet1/0
 redistribute connected
!
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 network 100.4.4.4 mask 255.255.255.255
 neighbor 10.1.1.13 remote-as 65001
 no auto-summary
!
ip access-list extended VENDOR
 permit tcp 192.168.32.0 0.0.7.255 host 10.199.100.1 eq 22 time-range VENDOR_ACCESS
!
time-range VENDOR_ACCESS
 periodic weekend 22:00 to 23:00
```

Refer to the exhibit. A network engineer received a call from the vendor for a failed attempt to remotely log in to their managed router loopback interface from 192.168.40.15. Which action must the network engineer take to resolve the issue?

A. The source IP summarization must be updated to include the vendor source IP address
B. The EIGRP configuration must be updated to include a network statement for loopback 100
C. The IP access list VENDOR must be applied to interface loopback 100
D. The time-range configuration must be changed to use absolute instead of periodic

Answer: A

QUESTION 39 

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

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

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

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

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

C.
```
control-plane
 no service-policy output PM-COPP
 service-policy input PM-COPPo access-list 100
```

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

Answer: A

QUESTION 40

```
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
```

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?

A. Modify the CoPP policy to increase the configured exceeded limit fro 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: C

Drag and Drop Questions

QUESTION 1 

Drag and drop the MPLS VPN device types from the left onto the definitions on the right.

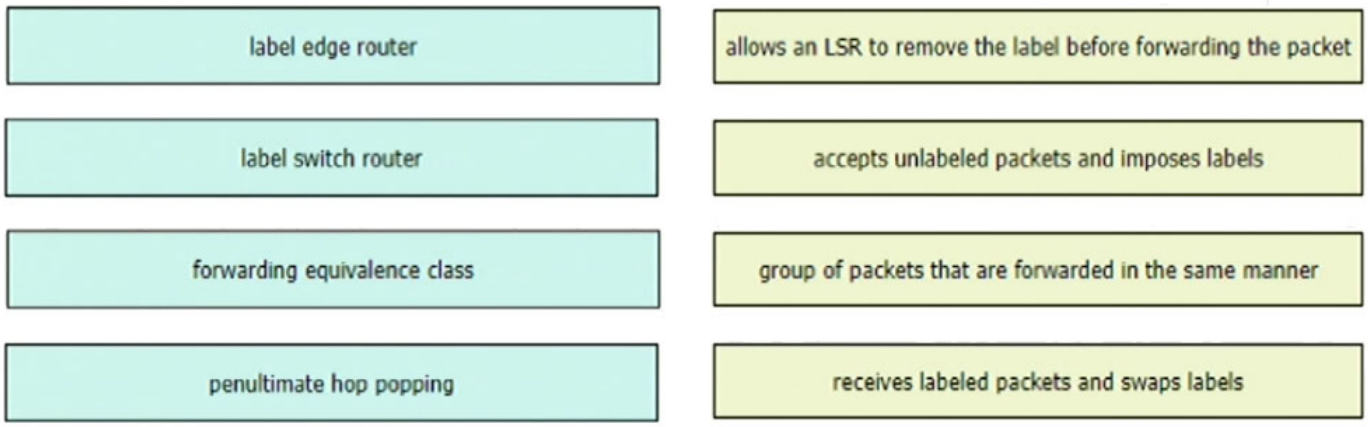
Customer (C) device	device in the core of the provider network that switches MPLS packets
CE device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device in the enterprise network that connects to other customer devices
Provider (P) device	device at the edge of the enterprise network that connects to the SP network

Answer:

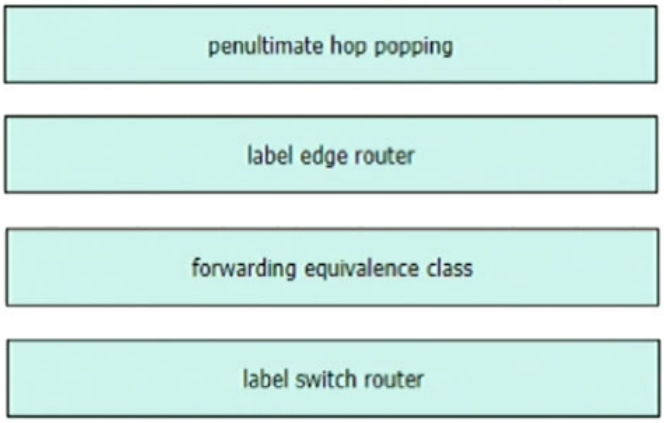
Provider (P) device	device in the core of the provider network that switches MPLS packets
PE device	device that attaches and detaches the VPN labels to the packets in the provider network
Customer (C) device	device in the enterprise network that connects to other customer devices
CE device	device at the edge of the enterprise network that connects to the SP network

QUESTION 2

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



Answer:

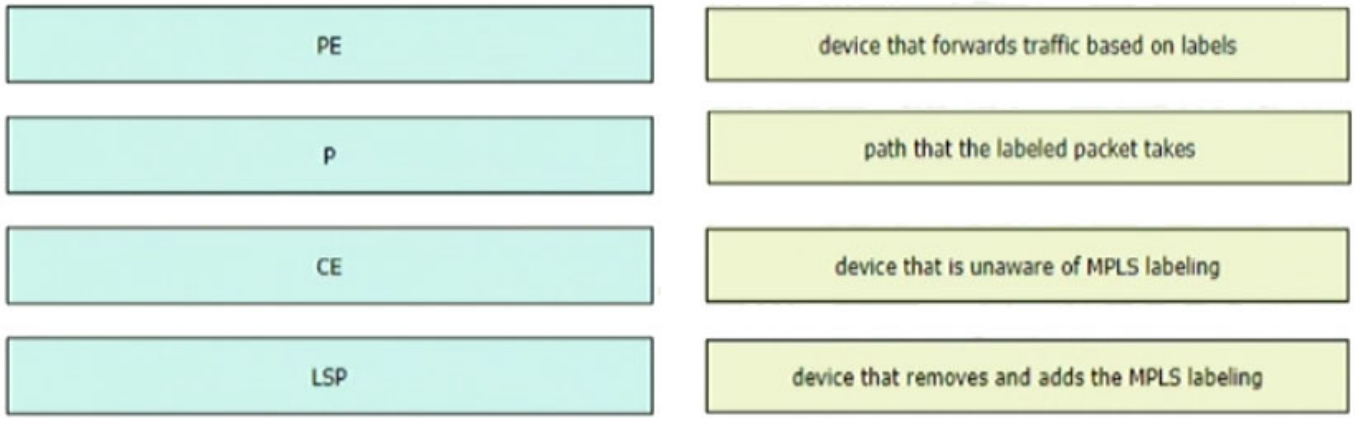


Explanation

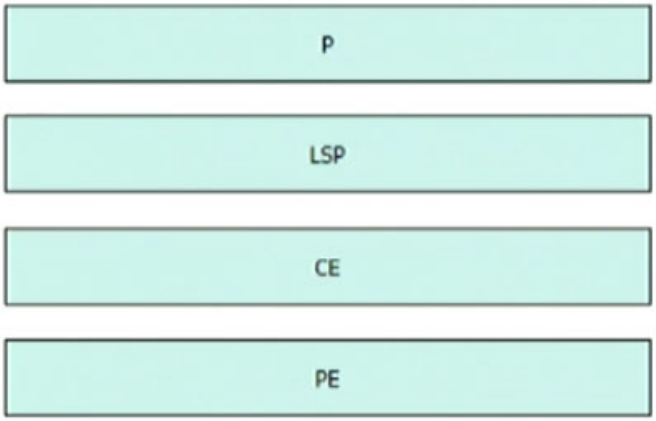
A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERs push an MPLS label onto an incoming packet and pop it off an outgoing packet. A forwarding equivalence class (FEC) is a term.

QUESTION 3

Drag and drop the MPLS terms from the left onto the correct definitions on the right.

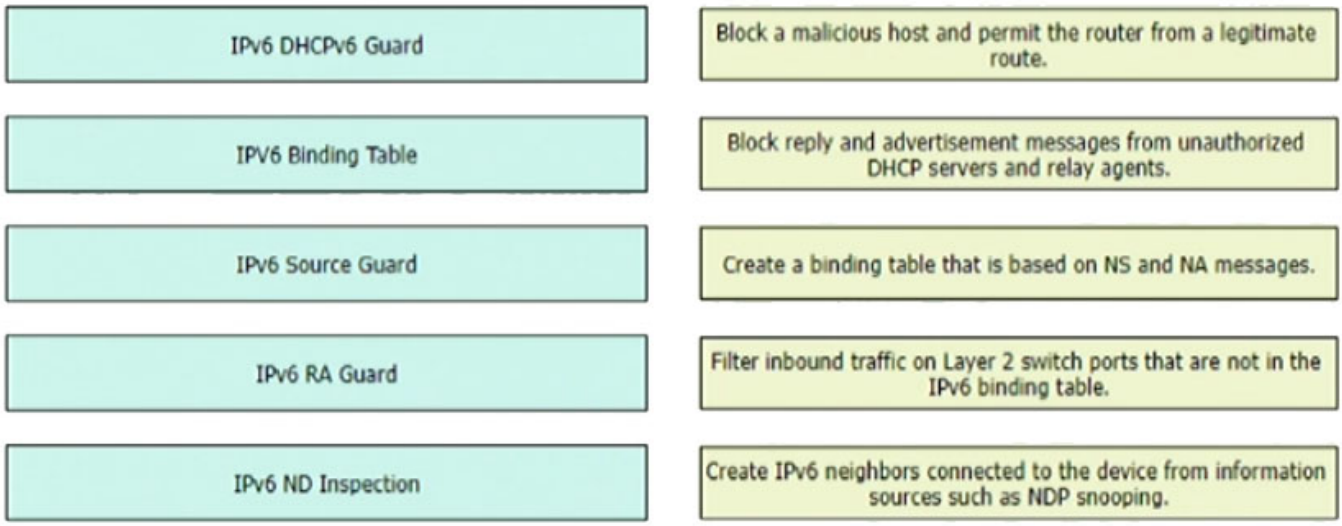


Answer:

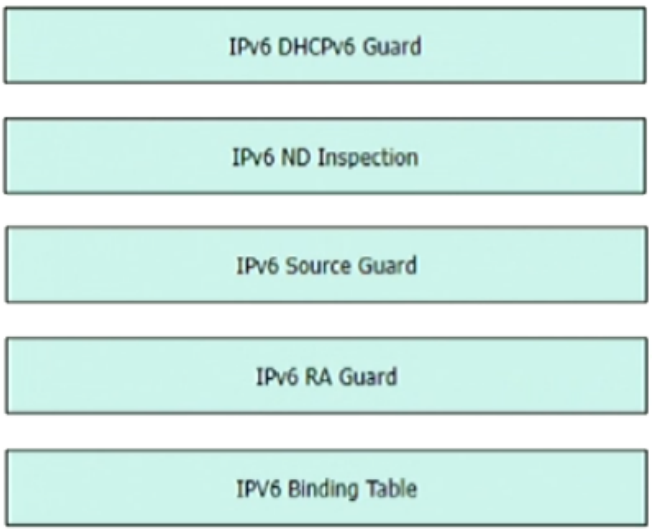


QUESTION 4

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

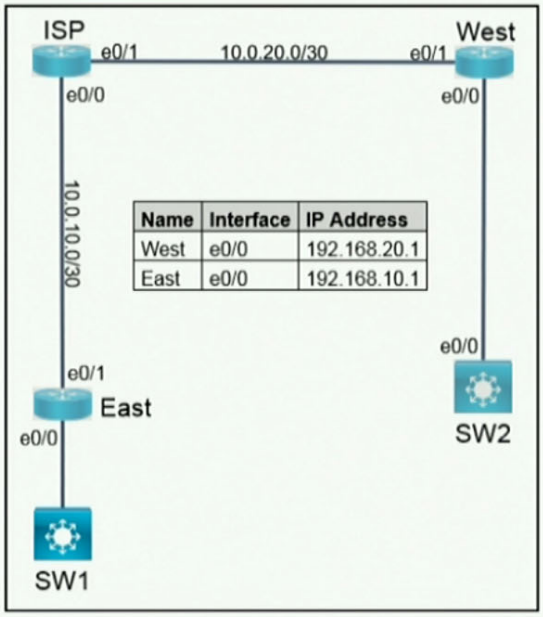


Answer:



Simulation 1 ☆☆☆☆

Guidelines | Topology | Tasks



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

ISP | East | West | SW2

```
ISP#
```

Guidelines | Topology | Tasks

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

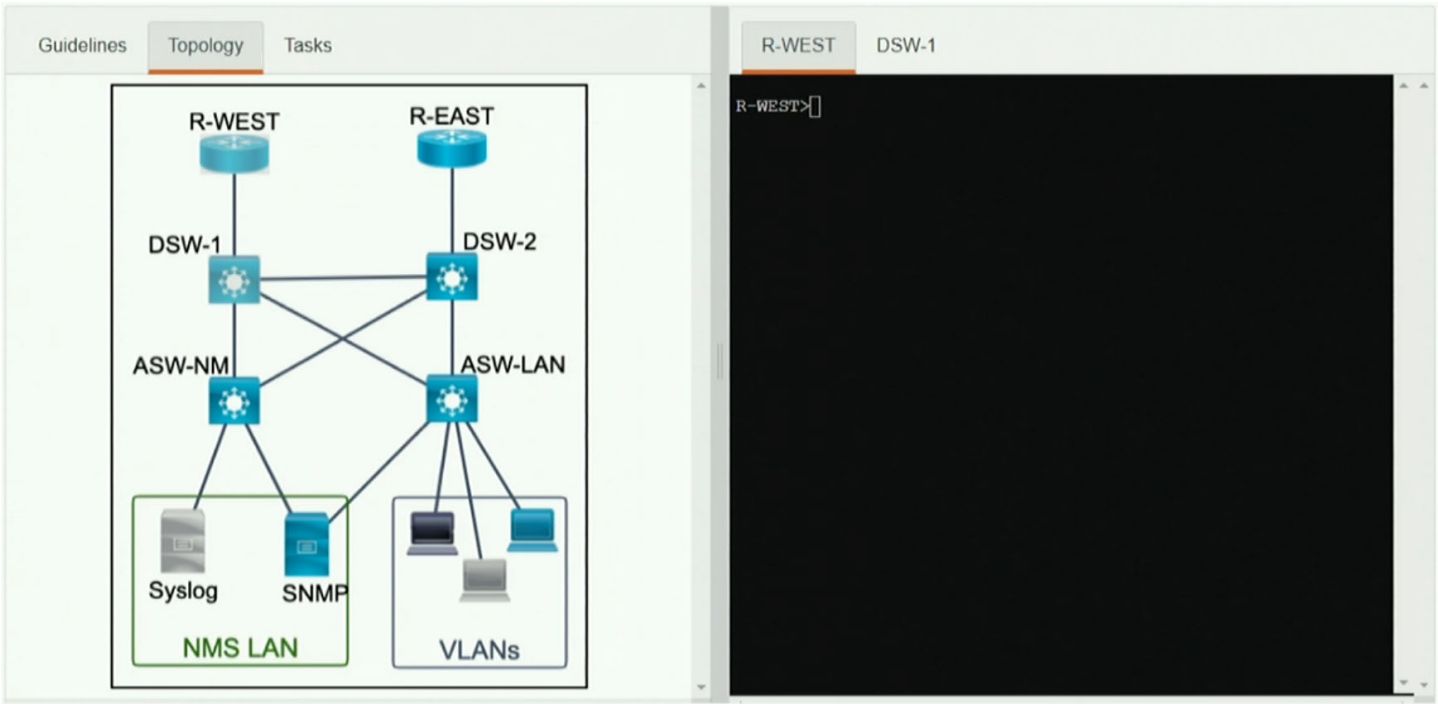
1. SW2 should only allow telnet access from ISP router's Loopback 0 using the AAA services. Fix the configs on SW2 to achieve this. Use preconfigured access-list ISP without removing the existing rule.
2. East router is configured to perform forwarding table lookup on an IP packet's source address, and 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.

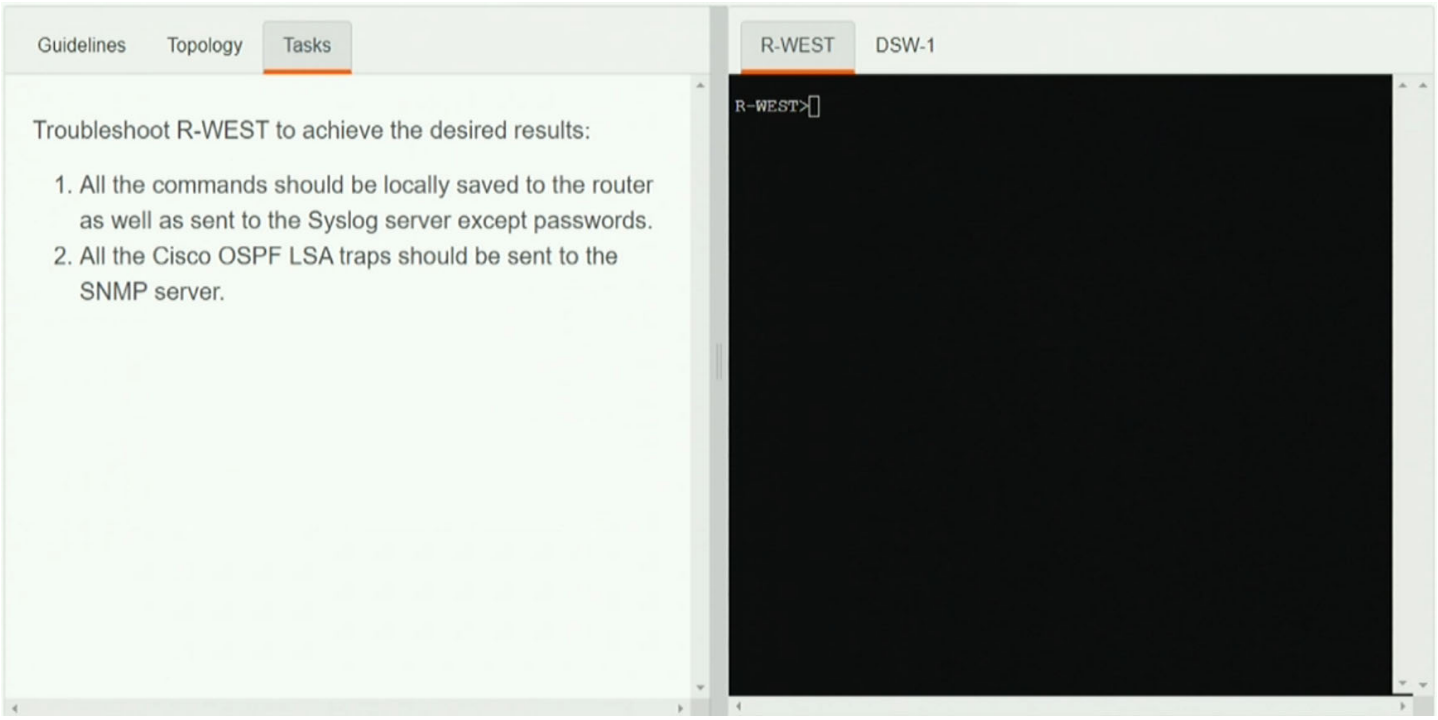
You must remove wrong preconfigs that have impact on tasks you are performing to fix issues.
Enable password is 'Cisco' on all devices
SW2: Local username is "SW2" and password is "Cisco"

ISP | East | West | SW2

```
ISP#
```

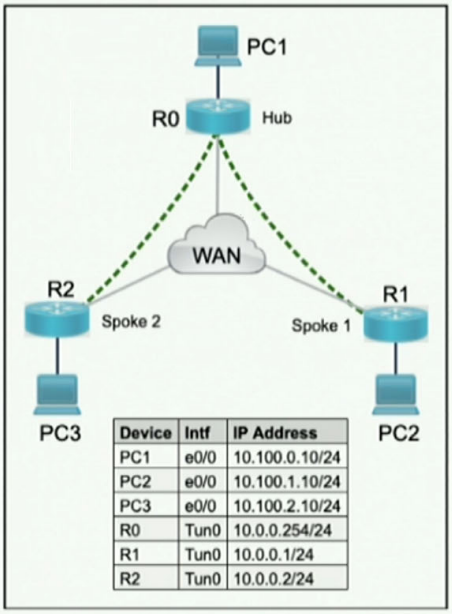
Simulation 2 ★★★★





Simulation 3 ☆☆☆☆

Guidelines | Topology | Tasks



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

PC1 | PC2 | PC3 | R0 | R1 | R2

```
PC1>
```

Guidelines | Topology | Tasks

Configure IPSec security policy on tunnel interfaces to ensure data confidentiality and integrity where mGRE tunnels are up and running between HUB and SPOKE routers.

1. Configure the ISAKMP policy parameters with the following attributes:
   - AES128
   - MD5
   - Group2
   - lifetime 86400
2. Ensure that GRE IP Header should not be encrypted inside the IPSec packet.
3. Configure a flexible ISAKMP Policy to add peers that have the dynamic IP addresses. Use a single command to configure it. Use IPSec phase-2 transform-set name as 'T-SET' and IPSec Profile name as 'T-SET-PROFILE'. Use ISAKMP key "abc123". Verify configuration with Ping from PC1 to PC2 and PC3.

PC1 | PC2 | PC3 | R0 | R1 | R2

```
PC1>
```