300-410$^{Q\&As}$

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

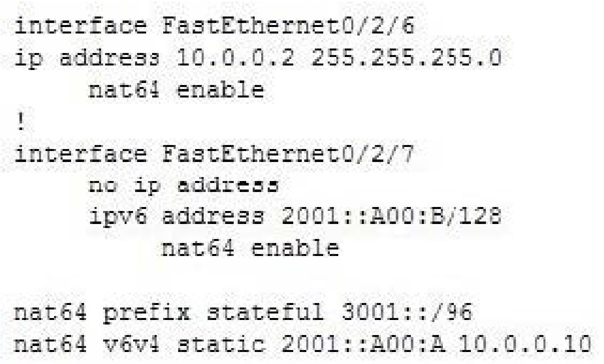
Pass Cisco 300-410 Exam with 100% Guarantee

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

You are configuring NAT64 to allow communication between a host running IPv6 and a server running IPv4. The router R1 sits between the host and the server. The router\\'s Fa0/2/7 interface is connected to the IPv6 host, and the Fa0/2/6 interface is connected to the IPv4 server.

The IPv6 host has an IPv6 address of 2001::a00:1/128 and the IPv4 server is at 10.0.0.1. Below is the relevant configuration on R1:



```
interface FastEthernet0/2/6
ip address 10.0.0.2 255.255.255.0
     nat64 enable
!
interface FastEthernet0/2/7
     no ip address
     ipv6 address 2001::A00:B/128
          nat64 enable

nat64 prefix stateful 3001::/96
nat64 v6v4 static 2001::A00:A 10.0.0.10
```

When the IPv4 server responds to the IPv6 host, what IPv6 address will be in the source address in the packet?

A. 2001::a001

B. 2001::A00:B

C. 3001::a00:1

D. 2001::A00:A

Correct Answer: C

NAT64 is a solution when IPv6 hosts need to communicate with IPv4-only servers. When the translation occur on the router the IPv4 address 10.0.0.1 will converted to hex as a00:1 and will be attached to the end of the stateful prefix of

3001::/96 that was configured on the router interface connected to the IPv4 server. The result will be 3001::a00:1.

The address will not be 2001::a001. The prefix that will be attached to the hex version of 10.0.0.1 will not be that of the interface fa0/2/7 but will be the prefix that was configured on that interface for nat64 translation which is 3301::/96. The

address will not be 2001::a00:b. That is the IPv6 address on the interface connected to the IPv6 host, but that address is not used for IPv4 to IPv6 communication. A translated address will be generated by converting the IPv4 address of the

IPv4 host to hex and attaching it to the IPv6 prefix configured on the interface connected to the IPv4 server.

The address will not be 2001::A00:A. That is the IPv6 address of the IPv6 host. That was statically mapped to 10.0.0.10 in the configuration and as such will be the IPv4 address used by the IPv6 host on the IPv4 side of the router.

Objective:

Infrastructure Services

Sub-Objective:

Describe IPv6 NAT

References:

Stateful Network Address Translation 64 (PDF)

QUESTION 2

You have configured OSPF on your network and enabled route summarization on an area border router (ABR) with the following command:

```
Router(config-router)# area 3 range 165.164.8.0 255.255.248.0
```

What does the 3 specify in this command?

A. The ID of the OSPF backbone

B. The number of networks summarized in the area

C. The ID of the area about which routes will be summarized

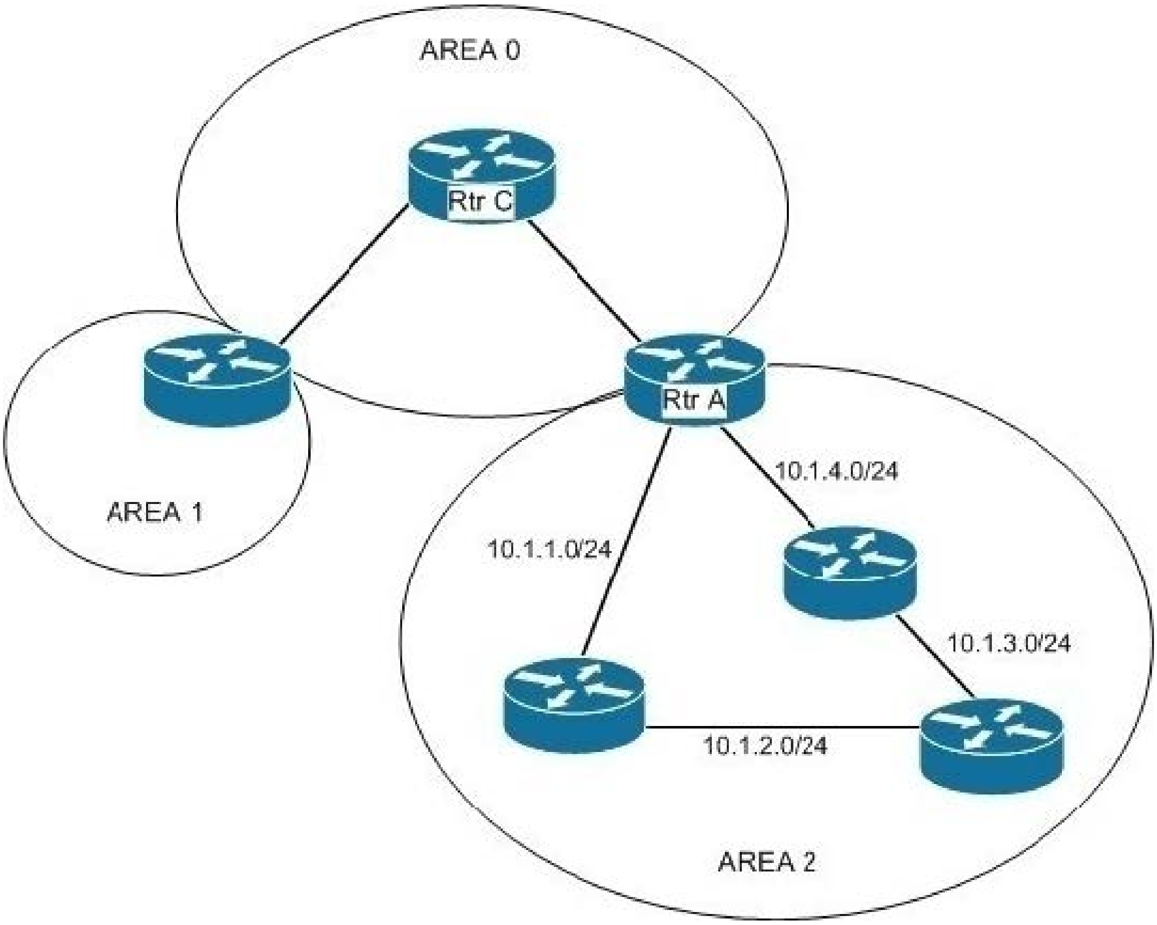
D. The ID of the area to which the summary route information will be sent

Correct Answer: C

The 3 in the area range command specifies the area that contains the routes that are to be summarized. In OSPF, you can only configure summarization on the border routers. The summaries need to be of routes within a single area. You summarize the routes of an area so that routers in another area do not see the individual networks, just the summary. The correct command syntax is shown below:

```
area number range ip-address mask
```

The number parameter is the number of the area whose networks are being summarized. For example, in the network shown in the graphic below, to summarize the networks within area 2 to 10.1.0.0/16, you would configure router A with the command area 2 range 10.1.0.0 255.255.0.0. This would not affect the routing tables of the routers within area 2, but instead make the routing tables of areas 0 and 1 smaller. These other routers would only have the summary route listed instead of the individual networks. Router C would only see the summary route 10.1.0.0/16.



Objective:

Layer 3 Technologies

Sub-Objective:

Configure and verify manual and autosummarization with any routing protocol References:

Cisco IOS Master Command Reference > a through b > area range

QUESTION 3

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

Correct Answer: CE

+

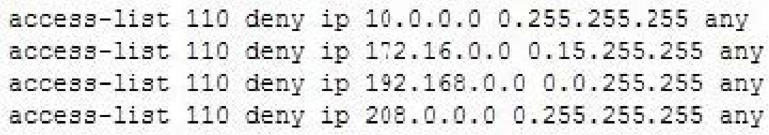
IGP: OSPF, EIGRP, IS-IS on core facing and core links+ RSVP and/or LDP on core and/or core facing links ->

+

MP-iBGP on PE devices (for MPLS services), MP-BGP: Multiprotocol Border Gateway Protocol, used for MPLS L3 VPN -> .

QUESTION 4

Examine the following access list: Which statement is NOT designed to prevent IP spoofing attacks from packets that appear to be sourced from inside the network, but are actually sourced from outside the network?



```
access-list 110 deny ip 10.0.0.0 0.255.255.255 any
access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
access-list 110 deny ip 208.0.0.0 0.255.255.255 any
```

A. access-list 110 deny ip 10.0.0.0 0.255.255.255 any

B. access-list 110 deny ip 172.16.0.0 0.15.255.255 any

C. access-list 110 deny ip 192.168.0.0 0.0.255.255 any

D. access-list 110 deny ip 208.0.0.0 0.255.255.255 any

Correct Answer: D

Infrastructure access control lists are designed to prevent spoofing attacks from packets that appear to be sourced from inside the network when they are in fact sourced from outside the network. There are two groups of address that should be blocked at the edge of the network: The private address space, which are called RFC 1918 addresses Certain "special use addresses" as defined in RFC 3330

The address 208.0.0.0 0.255.255.255 falls into neither of those categories.

The RFC 1918 addresses that should be blocked are:

10.0.0.0/24 172.16.0.0/16 192.168.0.0/16

The RFC 3330 addresses that should be blocked are:

0.0.0.0 127.0.0.0/8 192.0.2.0/24 224.0.0.0/4

For more information about these special use addresses, see RFC 3330.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify router security features

References:

Home > Support > Technology Support > IP > IP addressing services > Technology information > Technology white paper >Protecting Your Core: Infrastructure Protection Access Control Lists

QUESTION 5

Which table is used to map the packets in an MPLS LSP that exit from the same interface, via the same next hop, and have the same queuing policies?

A. RIB

B. FEC

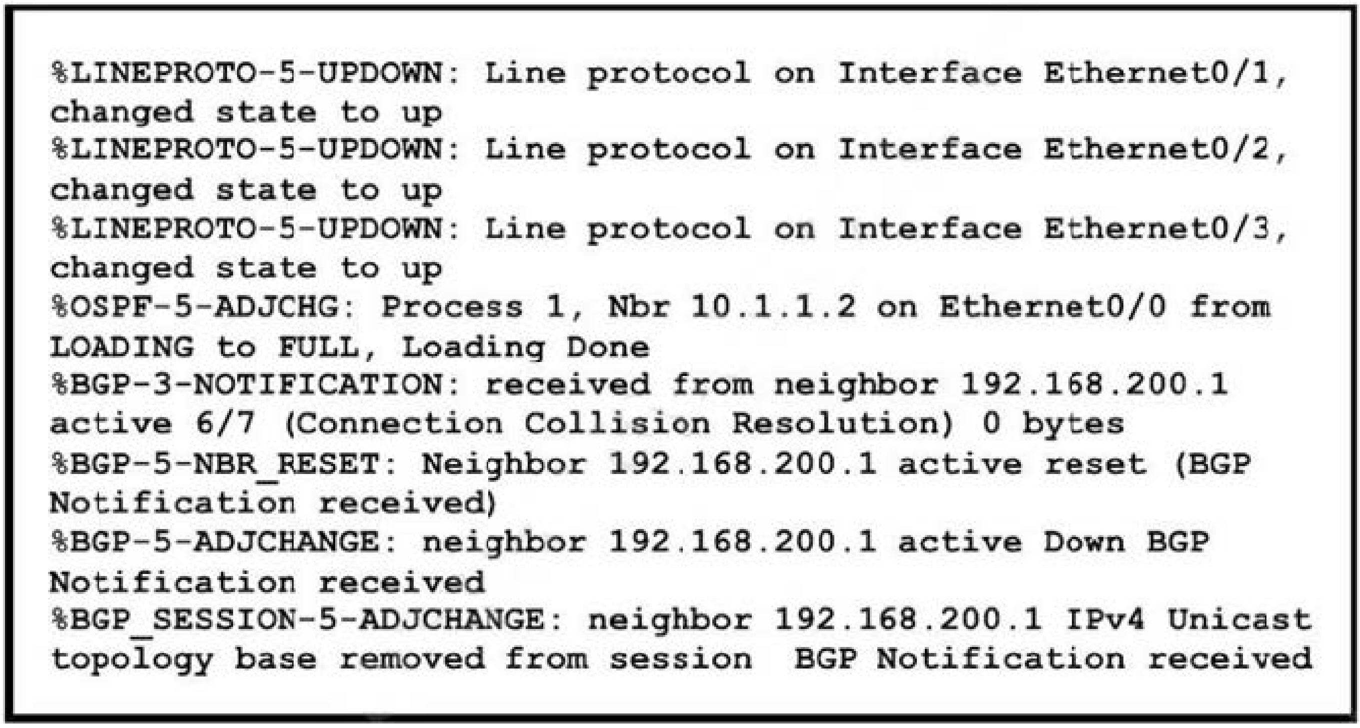
C. LDP

D. CEF

Correct Answer: B

QUESTION 6

Refer to the exhibit.



```
%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
```

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.

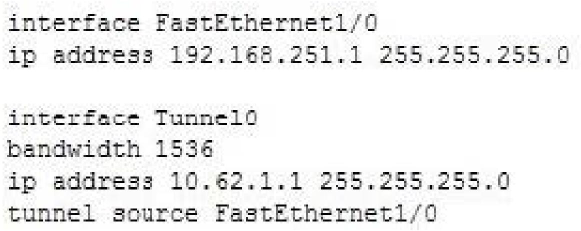
D. Configure the log uptime option.

Correct Answer: B

https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/service_timestamps.htm

QUESTION 7

You are troubleshooting an issue with the configuration of mGRE on the hub router in a hub-and-spoke configuration. Examine the output of the configuration of the tunnel interface on the hub router:



```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0

interface Tunnel0
bandwidth 1536
ip address 10.62.1.1 255.255.255.0
tunnel source FastEthernet1/0
```

Which of the following statements is true?

A. The tunnel destination must be specified on the tunnel interface

B. the tunnel mode gre multipoint command must be executed on the tunnel interface

C. the tunnel mode gre multipoint command must be executed on the physical interface

D. The tunnel destination must be specified on the physical interface

Correct Answer: B

The tunnel mode gre multipoint command must be executed on the tunnel interface. An mGRE configuration is one in which the tunnel is allowed to have multiple destinations. The distinguishing feature between an mGRE interface and a

point-to-point GRE interface is the tunnel destination. While it is specified on a point-to-point GRE interface, it is not on an mGRE interface. Instead the command tunnel mode gre multipoint is executed on the tunnel interface. This allows the

interface to use the Next Hop Routing protocol (NHRP) to discover the IP addresses of the other tunnel endpoints.

The tunnel destination is not specified on the tunnel interface using mGRE. Instead the command tunnel mode gre multipoint is executed on the tunnel interface.

The tunnel mode gre multipoint command must be executed on the tunnel interface, not the physical interface. The tunnel destination is neither specified on the tunnel interface nor on the physical interface when using mGRE.

Objective:

VPN Technologies

Sub-Objective:

Configure and verify GRE

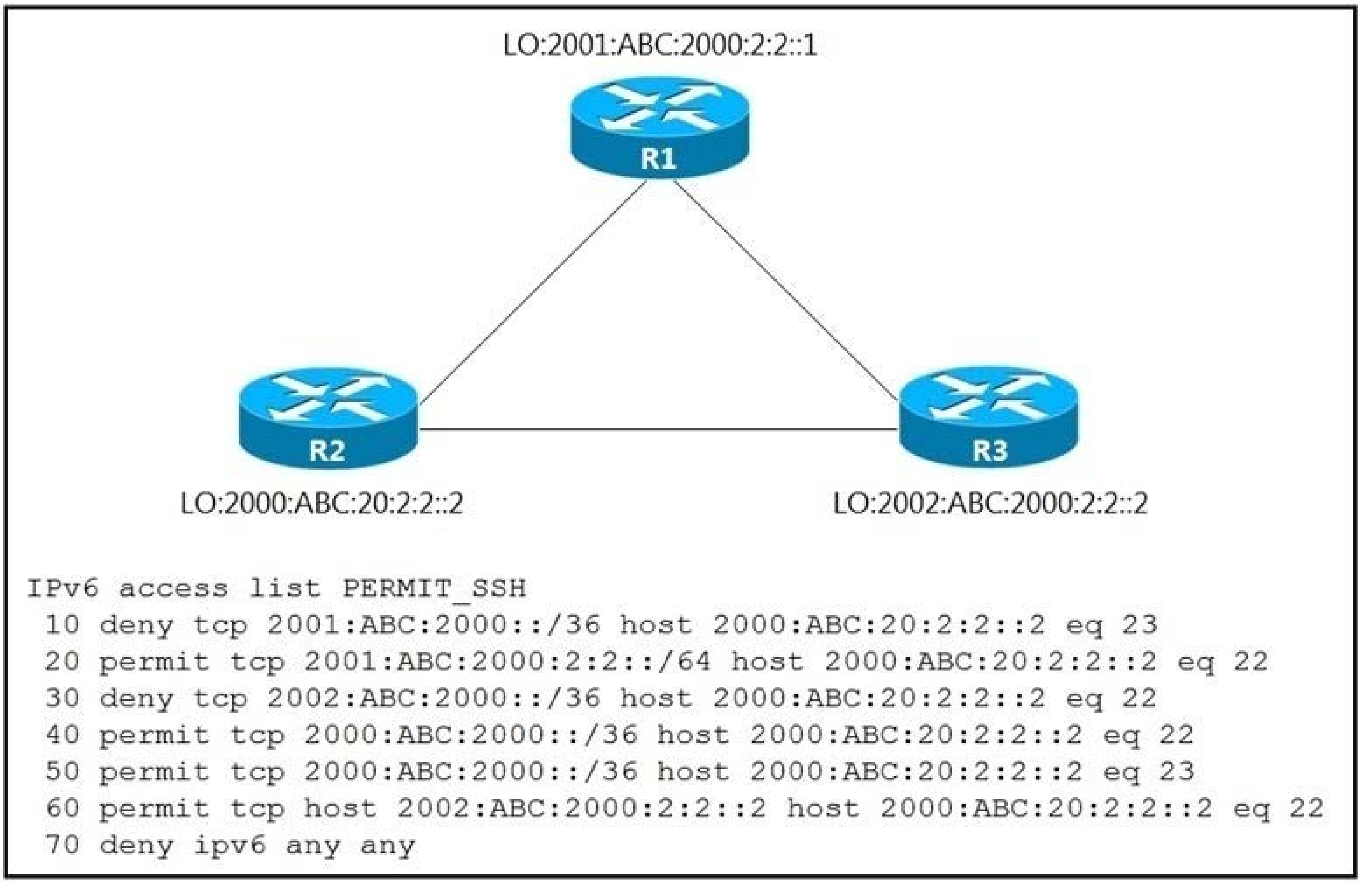
References:

Cisco > Dynamic Multipoint VPN (DMVPN) Design Guide (Version 1.1) > DMVPN Design and Implementation > mGRE Configuration

Cisco > Cisco IOS IP Mobility Command Reference > tunnel mode gre

QUESTION 8

Refer to the exhibit.



```
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
```

An IPv6 network was newly deployed in the environment and the help desk reports that R3 cannot SSH to the R2s Loopback interface. Which action resolves the issue?

A. 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.

Correct Answer: C

QUESTION 9

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 Guard

B. DHCPv6 Root Guard

C. IPv6 Source Guard

D. IPv6 Prefix Guard

Correct Answer: CD

QUESTION 10

There is an issue between two nodes within your network, and you are using Cisco DNA Center Path Trace to help troubleshoot the problem. Which of the following statements are true regarding the Path Trace tool?

A. Overlapping IP addresses are supported.

B. Path trace between a fabric client and a non-fabric client is supported

C. Path trace between a wired client and a wireless client is supported

D. Only TCP traffic is supported.

Correct Answer: C

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-2-2/b_cisco_dna_assurance_2_2_2_ug/b_cisco_dna_assurance_2_2_2_ug_chapter_01111.html

QUESTION 11

Which of the following are valid restrictions when configuring Control Plane Policing (CoPP) on Cisco devices? (Choose two.)

A. You cannot use the "log" keyword with CoPP on the access list entries

B. CEF must be disabled

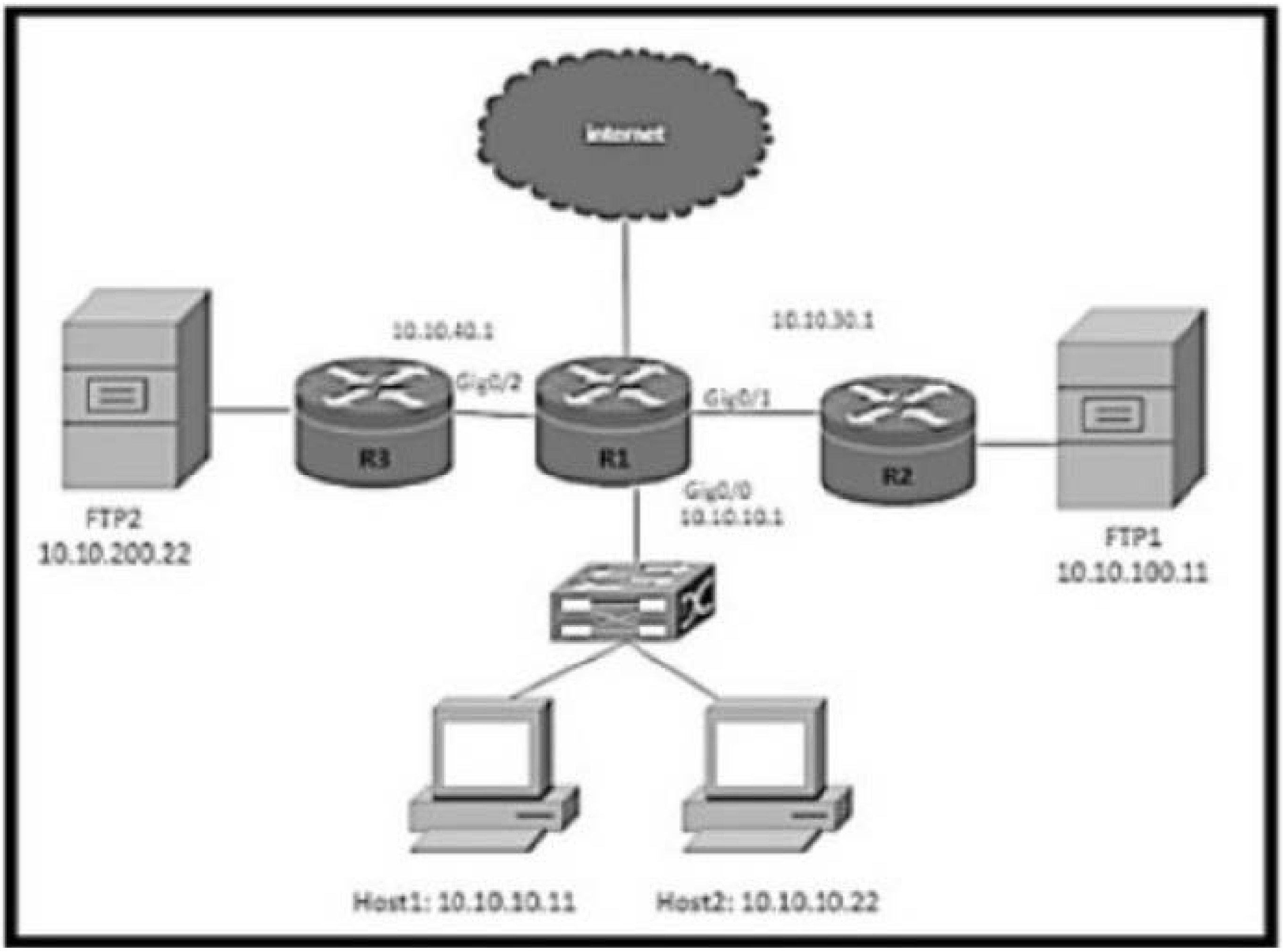
C. The only match types supported with CoPP is ip precedence, ip dscp, and access-group

D. Only standard access-lists are supported.

Correct Answer: AC

QUESTION 12

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:

1.

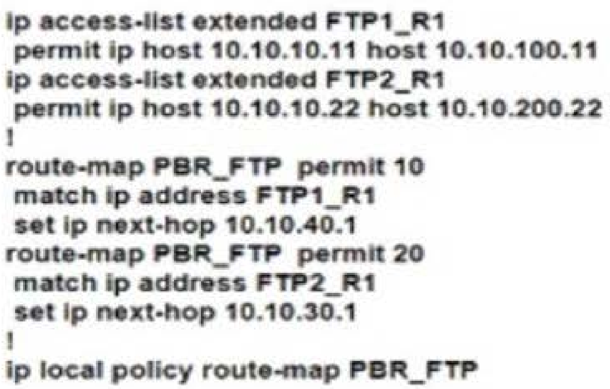
Host1 must use the FTP1 fileserver.

2.

Host2 must use the FTP2 fileserver.

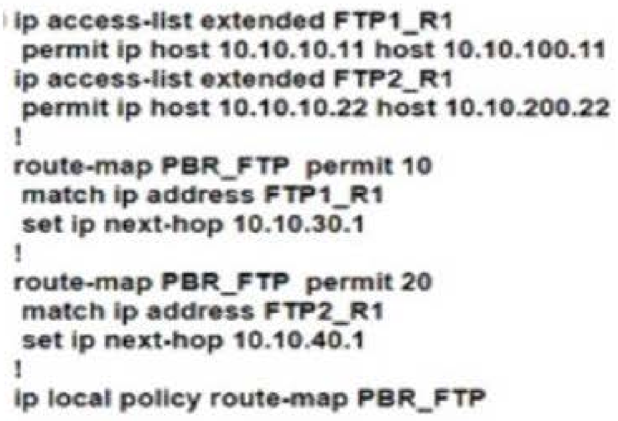
Which configuration meets the requirement on R1?

A.



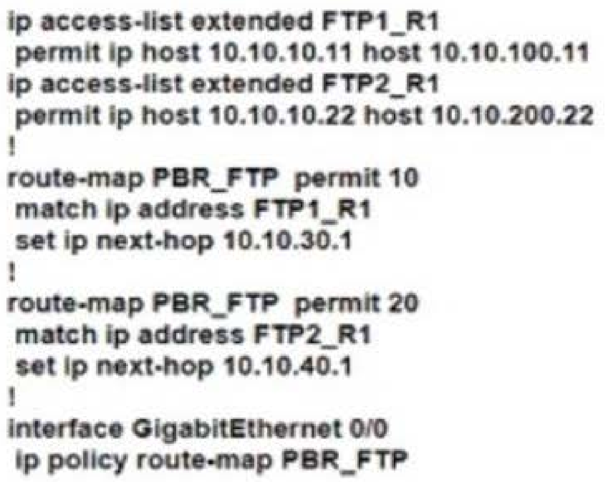
```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.40.1
route-map PBR_FTP  permit 20
 match ip address FTP2_R1
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

B.



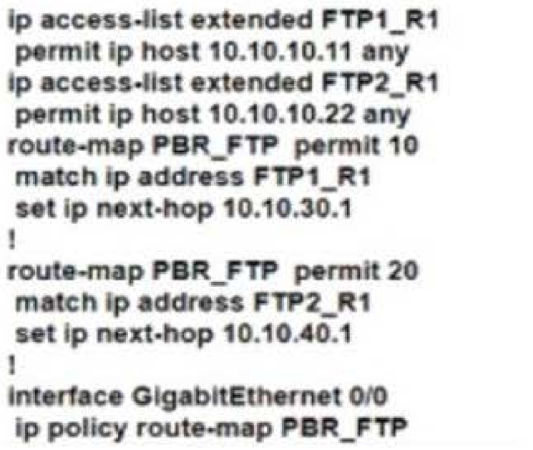
```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 host 10.10.100.11
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 host 10.10.200.22
!
route-map PBR_FTP  permit 10
 match ip address FTP1_R1
 set ip next-hop 10.10.30.1
!
route-map PBR_FTP  permit 20
 match ip address FTP2_R1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



```
ip access-list extended FTP1_R1
 permit ip host 10.10.10.11 any
ip access-list extended FTP2_R1
 permit ip host 10.10.10.22 any
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
```

A. Opiton A

B. Opiton B

C. Opiton C

D. Opiton D

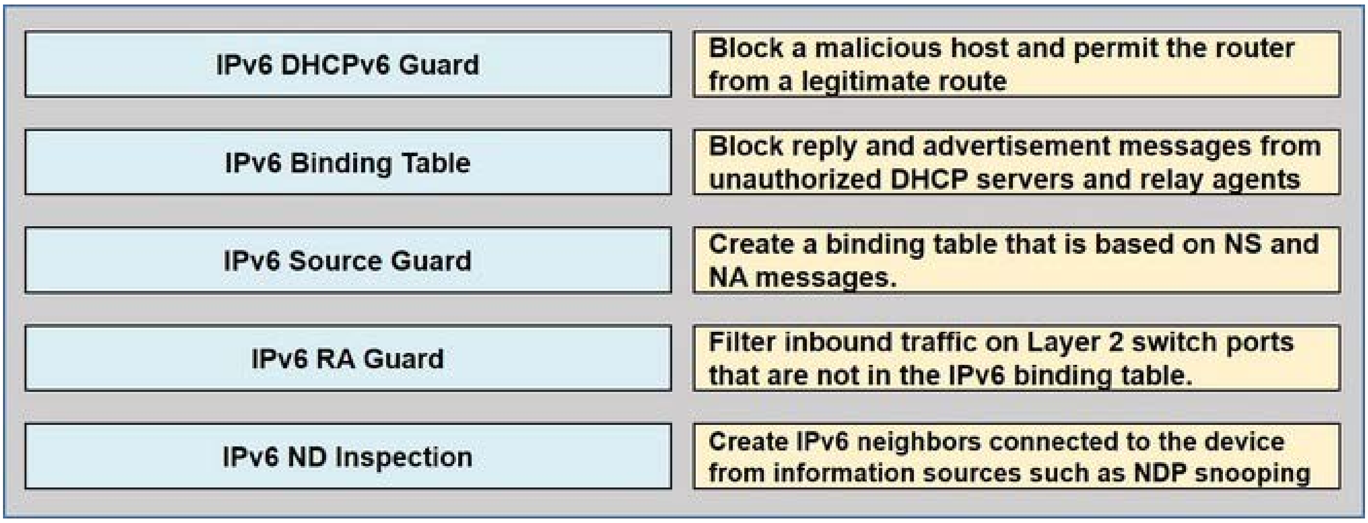
Correct Answer: C

QUESTION 13

DRAG DROP

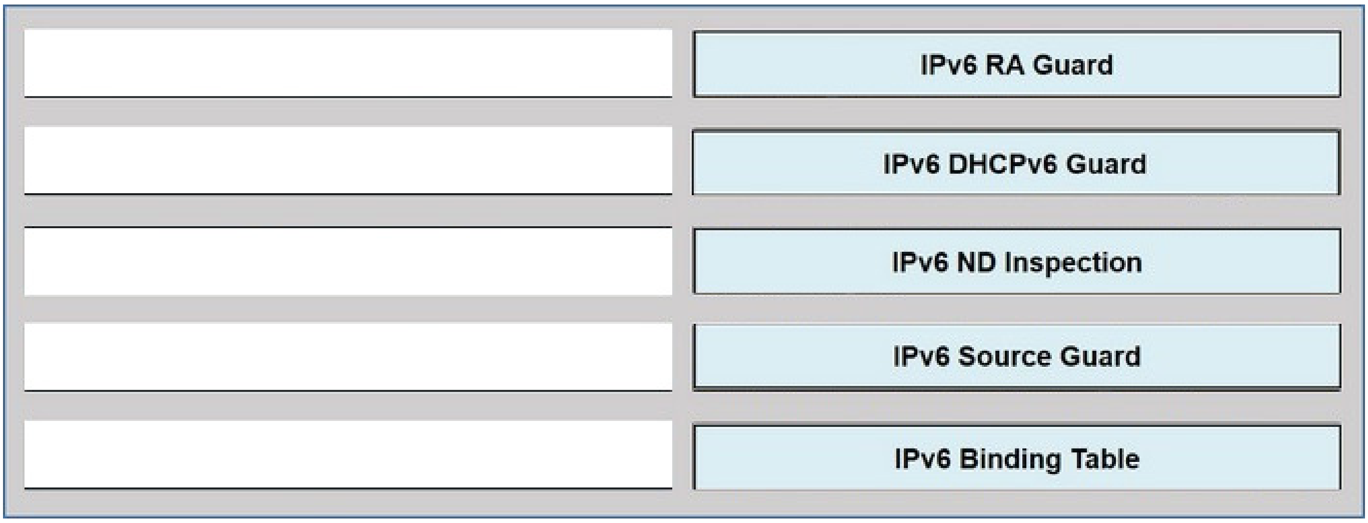
Drag and Drop the IPv6 First-Hop Security features from the left onto the definitions on the right.

Select and Place:



IPv6 DHCPv6 Guard	Block a malicious host and permit the router from a legitimate route
IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents
IPv6 Source Guard	Create a binding table that is based on NS and NA messages.
IPv6 RA Guard	Filter inbound traffic on Layer 2 switch ports that are not in the IPv6 binding table.
IPv6 ND Inspection	Create IPv6 neighbors connected to the device from information sources such as NDP snooping

Correct Answer:



	IPv6 RA Guard
	IPv6 DHCPv6 Guard
	IPv6 ND Inspection
	IPv6 Source Guard
	IPv6 Binding Table

+

Block reply and advertisement messages from unauthorized DHCP servers and relay agents: IPv6 DHCPv6 Guard

+

Create a binding table that is based on NS and NA messages: IPv6 ND Inspection

+

Filter inbound traffic on Layer 2 switch port that are not in the IPv6 binding table: IPv6 Source Guard

+

Block a malicious host and permit the router from a legitimate route: IPv6 RA Guard

+

Create IPv6 neighbors connected to the device from information sources such as NDP snooping: IPv6 Binding Table

QUESTION 14

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

A. LSP

B. RSVP

C. ECMP

D. LDP

E. MPLS OAM

Correct Answer: BD

QUESTION 15

Which of the following are commonly used ports when implementing RADIUS based authentication and accounting? (Choose two.)

A. UDP port 1644 for authentication

B. UDP port 1812 for authentication

C. TCP port 1812 for authentication

D. UDP port 1813 for accounting

E. TCP port 1813 for accounting

F. UDP port 1644 for accounting

Correct Answer: BD