# Free Questions for 300-410 by vceexamstest

## Shared by Beck on 06-06-2022

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

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

## Options:

**A-** RA Throttling

**B-** Source or Destination Guard

**C-** ND Multicast Suppression

**D-** IPv6 Snooping

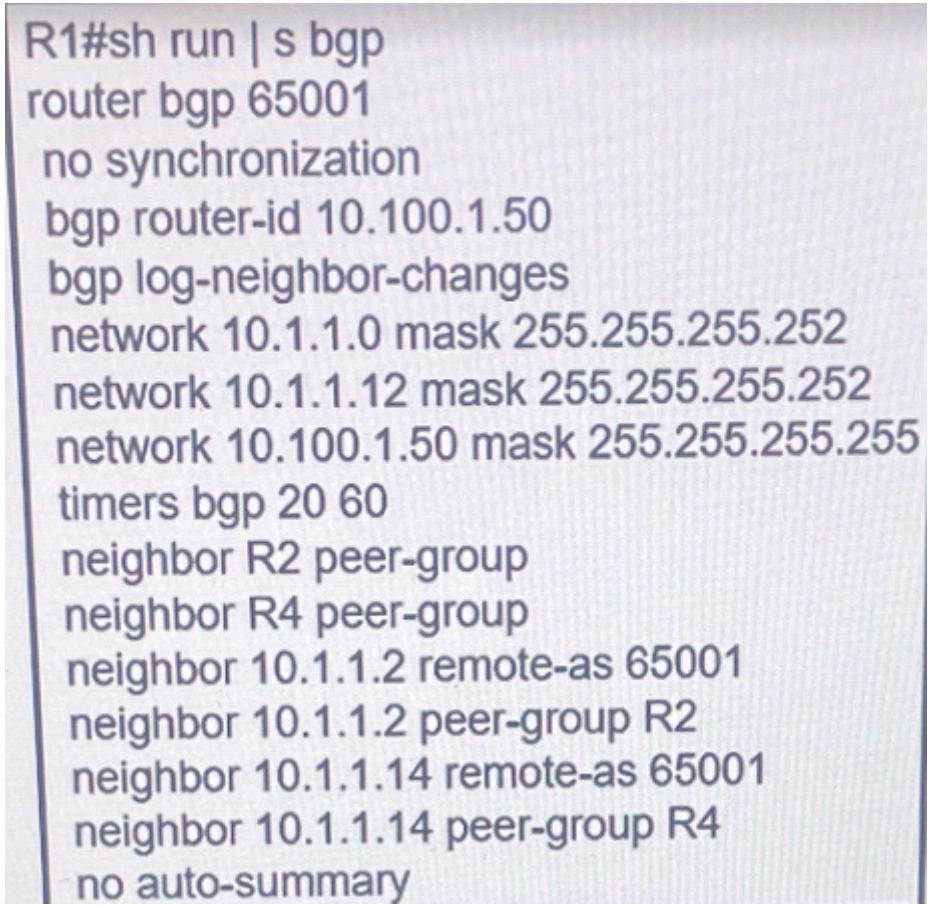
## Answer:

D

# Question 2

**Question Type:** MultipleChoice

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)

## Options:

**A-** neighbor 10.1.1.14 route-reflector-client

**B-** neighbor R2 route-reflector-client

**C-** neighbor 10.1.1.2 allowas-in

**D-** neighbor R4 route-reflector-client

**E-** neighbor 10.1.1.2 route-reflector-client

## Answer:

A, E

# Question 3

**Question Type:** **MultipleChoice**

An engineer configured a router with this configuration

ip access-hst DENY TELNET

10 deny tcp any any eq 23 log-input

The router console starts receiving log message :%SEC-6-IPACCESSLOGP: list DENY_TELNET denied tcp 192.168.1.10(1022)(FastEthernet1/0 D508.89gb.003f) ->192.168.2.20(23), 1 packet"

Which action stops messages on the console while still denying Telnet?

### Options:

**A-** Configure a 20 permit ip any any command

**B-** Remove log-Input keyword from the access list.

**C-** Replace log-input keyword with the log keyword in the access list.

**D-** Configure a 20 permit ip any any log-input command.

### Answer:

B

## Question 4

**Question Type:** **MultipleChoice**

What are the two goals of micro BFD sessions? (Choose two.)

## Options:

**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:

C, E

## Explanation:

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

# Question 5

**Question Type:** MultipleChoice

What is a function of an end device configured with DHCPv6 guard?

## Options:

**A-** If it is configured as a server, only prefix assignments are permitted.

**B-** If it is configured as a relay agent, only prefix assignments are permitted.

**C-** If it is configured as a client, messages are switched regardless of the assigned role.

**D-** If it is configured as a client, only DHCP requests are permitted.

## Answer:

C

## Explanation:

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized

DHCP servers and relay agents.

Packets are classified into one of the three DHCP type messages. All client messages are always

switched regardless of device role. DHCP server messages are only processed further if the device role

is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes).

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

# Question 6

**Question Type:** MultipleChoice

What are the two prerequisites to enable BFD on Cisco routers? (Choose two)

## Options:

**A-** A supported IP routing protocol must be configured on the participating routers.

**B-** OSPF Demand Circuit must run BFD on all participating routers.

**C-** ICMP must be allowed on all participating routers.

**D-** UDP port 1985 must be allowed on all participating routers.

**E-** Cisco Express Forwarding and IP Routing must be enabled on all participating routers.

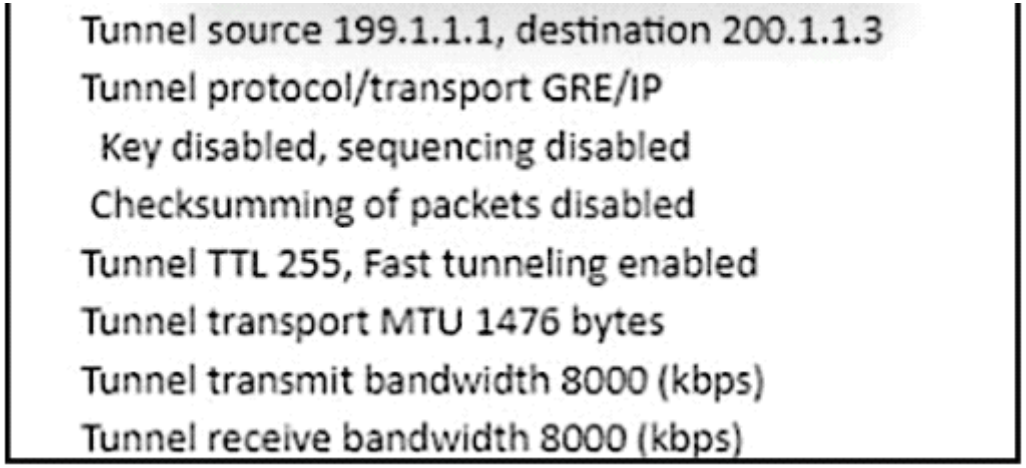
### Answer:

C, E

## Question 7

**Question Type:** **MultipleChoice**

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?

## Options:

**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

# Question 8

**Question Type:** MultipleChoice

Refer to the exhibit.

```
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 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?

## Options:

**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:

B

# Question 9

**Question Type:** MultipleChoice

Refer to the exhibit.

```
R1#sh ip route
     10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

Although summarization is configured for R1 to receive 10.0.0.0/8. more specific routes are received by R1. How should the 10.0.0.0/8 summary route be received from the neighbor, attached to R1 via Fast Ethernet0/0 interface?

## Options:

**A-** R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0.255.0.0.0 command under the Fast Ethernet 0/0 interface.

**B-** The summarization condition is not met Router 10 1 100.10 requires a route for 10 0.0.0/8 that points to null 0

**C-** The summarization condition is not met. The network 10.1.100.0/24 should be changed to 172.16.0.0/24.

**D-** R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0 0.0.0.255 command under the Fast Ethernet 0/0 interface.

## Answer:

D

# Question 10

**Question Type:** MultipleChoice

What does the MP-BGP OPEN message contain?

## Options:

**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

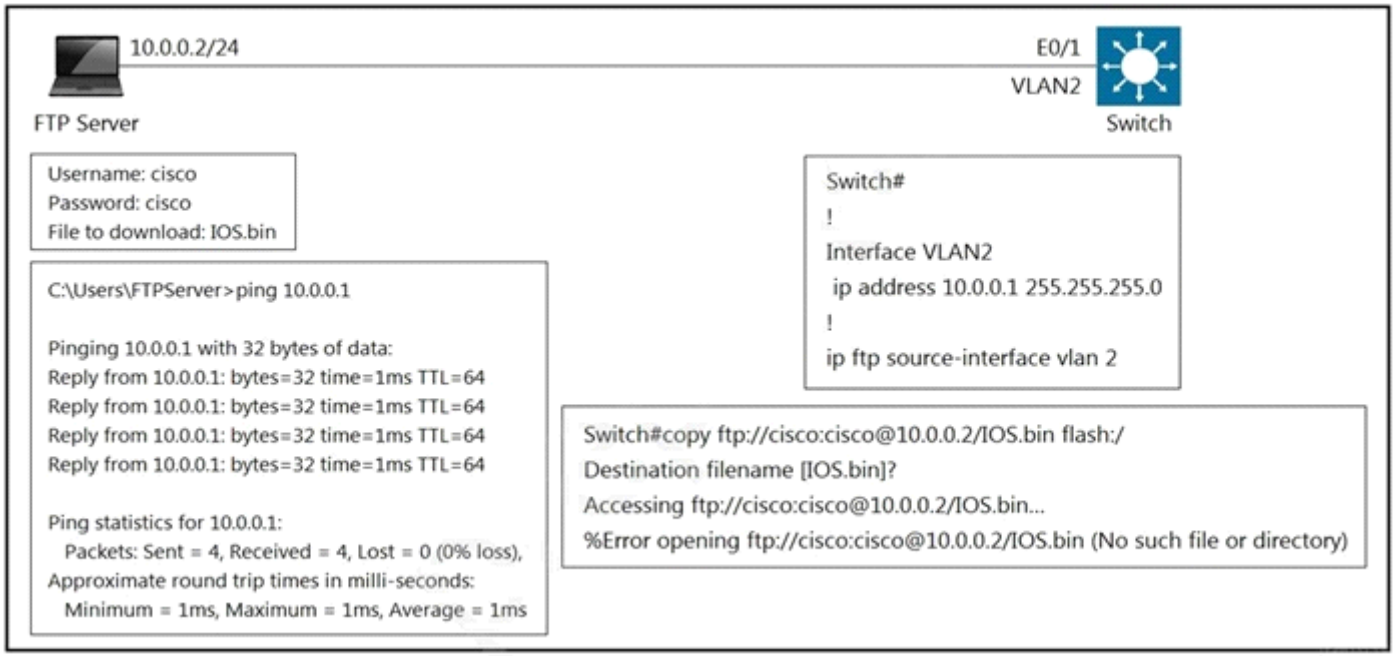
### Answer:

B

# Question 11

**Question Type:** **MultipleChoice**

Refer to the exhibit.




An engineer cannot copy the IOS.bin file from the FTP server to the switch.

Which action resolves the issue?

## Options:

**A-** Allow file permissions to download the file from the FTP server.

**B-** Add the IOS.bin file, which does not exist on FTP server.

**C-** Make memory space on the switch flash or USB drive to download the file.

**D-** Use the copy flash:/ ftp://cisco@10.0.0.2/IOS.bin command.

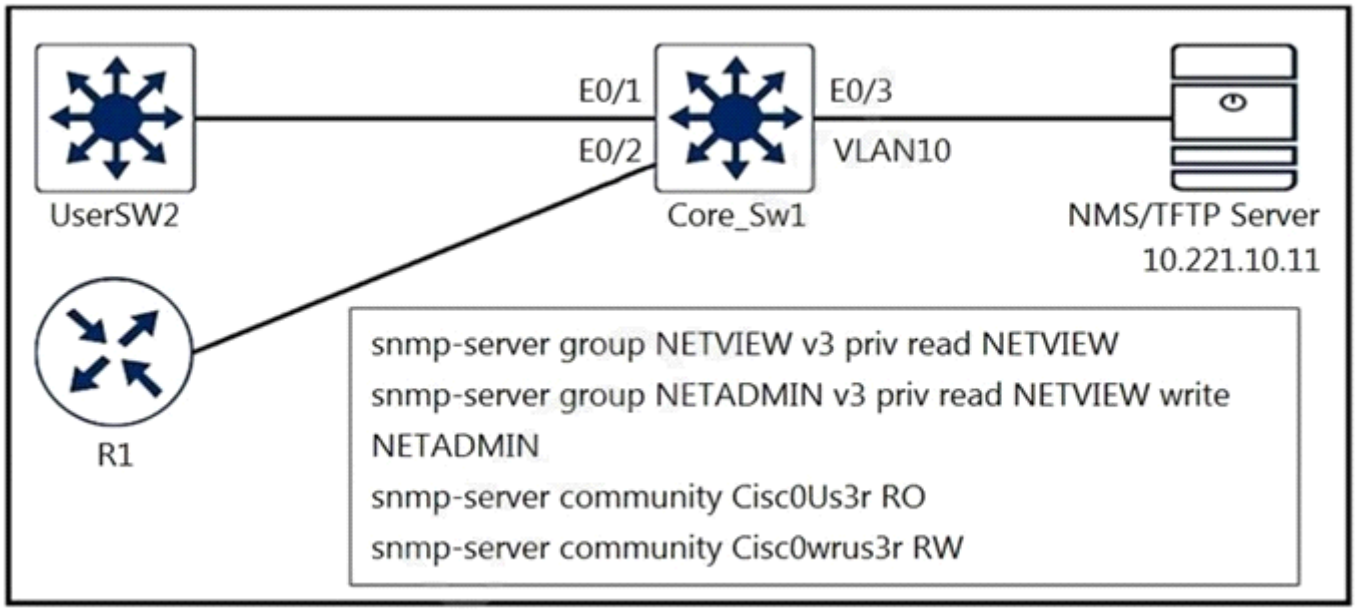
### Answer:

B

# Question 12

**Question Type:** **MultipleChoice**

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?

## Options:

**A-** 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

**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

**D-** access-list 20 permit 10.221.10.11

## Answer:

A