Free Questions for 300-410 by certsdeals

Shared by Santiago on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A) Configure EIGRP to receive 192.168.32.0 route with lower admin distance.

B) A. Configure EIGRP to receive 192.168.32.0 route with longer prefix than /19.

C) A. Configure EIGRP to receive 192.168.32.0 route with lower metric.

D) A. Configure EIGRP to receive 192.168.32.0 route with equal or longer prefix than /24.

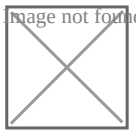
Answer:

D

Question 2

Question Type: MultipleChoice

Exhibit:



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

(Choose two)

Options:

A) Configure BGP in the COPP-CRITICAL-7600 ACL

B) Configure a higher value for CIR under the default class to allow more packets during peak traffic

C) Configure a higher value for CIR under the class COPP-CRITICAL-7600

D) Configure a three-color policer instead of two-color policer under class COPP-CRITICAL-7600

E) Configure IP CEF to CoPP policy and BGP to work

Answer:

A, B

Explanation:

The policy-map COPP-7600 only rate-limit HTTP & HTTPS traffic (based on the ACL

conditions) so any BGP packets will be processed in the class "class-default", which drops

exceeded BGP packets. Therefore we have two ways to solve this problem:

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

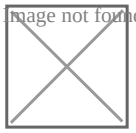
+ Configure higher value for CIR in default class as 2Mbps is too low for web traffic (http &

https)

Question 3

Question Type: MultipleChoice

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



Options:

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

B) Configure DSW1(dhcp-config)#default-router 2002:A04:A01::A04:A01

C) Configure DSW1(config)#ipv6 route 2002:404:404:404:404/128 FastEthernet1/0

D) Configure DSW1(config-if)#ipv6 dhcp relay destination 2002:404:404::404:404 GigabitEthernet1/2

Answer:

B

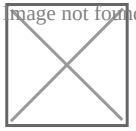
Explanation:

https://community.cisco.com/t5/networking-documents/stateful-dhcpv6-relay-configuration-example/ta-p/3149338

Question 4

Question Type: MultipleChoice

Exhibit:



Bangkok is using ECMP to reach to the 192.168.5.0/24 network. The administrator must configure Bangkok in such a way that Telnet traffic from 192.168.3.0/24 and192.168.4.0/24 networks uses the HongKong router as the preferred router. Which set of configurations accomplishes this task?

Options:

A) access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
interface Ethernet0/3
ip policy route-map PBR1

B) access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23

!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
interface Ethernet0/1
ip policy route-map PBR1

C) access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
!
interface Ethernet0/3
ip policy route-map PBR1

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

Answer:

C

Explanation:

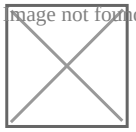
We need to use Policy Based Routing (PBR) here on Bangkok router to match the traffic from 192.168.3.0/24 & 192.168.4.0/24 and "set ip next-hop" to HongKong router(172.18.1.2 in this case).

Note: Please notice that we have to apply the PBR on incoming interface e0/3 to receive traffic from 192.168.3.0/24 and 192.168.4.0/24.

Question 5

Question Type: MultipleChoice

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?

Options:

A) R1 and R4

B) R1 and R5

C) R4 and R5

D) R2 and R5

Answer:

C

Explanation:

When R2 & R5 are route reflectors (RRs), routes from R4 & R8 are advertised to R5 and R5

advertises to R2. But R2 would drop them as R2 is also a RR. Therefore some routes are

missing on R1 to advertise to eBGP peers.

Good reference:

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/TECRST-2310.pdf

Route reflectors (RR) must be fully iBGP meshed so we cannot configure RR on both R1 and

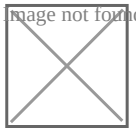
R5.

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

Question 6

Question Type: **MultipleChoice**

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?

Options:

A) Check and resolve reachability between the WLC and the NTP server

B) Reset the NTP server to resolve any synchronization issues for all devices

C) Check and resolve reachability between Cisco DNA Center and the NTP server

D) Check and configure NTP on the WLC and synchronize with Cisco DNA Center

Answer:

D

Explanation:

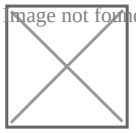
Excessive time lag between Cisco DNA Center and device: The time difference between Cisco DNA Center and the device IP Address has drifted too far apart. CiscoDNA Center cannot process the device data accurately if the time difference is more than 3 minutes.

Question 7

Question Type: **MultipleChoice**

A network administrator is trying to access a branch router using TACACS+ username and password credentials, but the administrator cannot log in to the router because the WAN connectivity is down. The branch router has following AAA configuration:

Image not found or type unknown



Which command will resolve this problem when WAN connectivity is down?

Options:

A) aaa authentication login default group tacacs+ local

B) aaa authentication login default group tacacs+ enable

C) aaa authentication login default group tacacs+ console

D) aaa authentication login console group tacacs+ enable

Answer:

A

Explanation:

With the "aaa authentication login default group tacacs+ local " command configured, when logging in, the password supplied will be attempted to be verified by the TACACS+ server before access is granted. If the server is unavailable/unreachable, then the switch will fall back to using the local authentication database.

Question 8

Question Type: MultipleChoice

Refer to the exhibit. A network engineer receives a report that Spoke 1 users can perform bank transactions with the server located at the Center site, but Spoke 2 users cannot. Which action resolves the issue?

Options:

A) Configure the Spoke 2 users IP on the router B OSPF domain

B) Configure encapsulation dot1q 78 on the router C interface.

C) Configure IPv6 on the routers B and C interfaces

D) Configure OSPFv2 on the routers B and C interfaces

Answer:

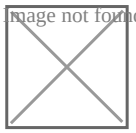
C

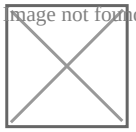
Question 9

Question Type: MultipleChoice

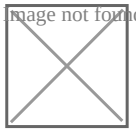
LAB SIMULATION

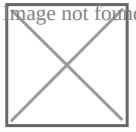
A network is configured with CoPP to protect the CORE router route processor for stability and DDoS protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:

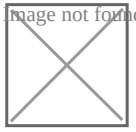




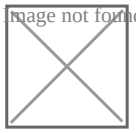
WAN

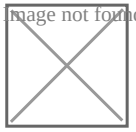


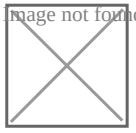


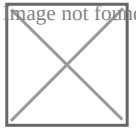


CORE

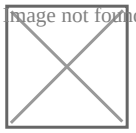


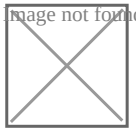






MGMT





Options:

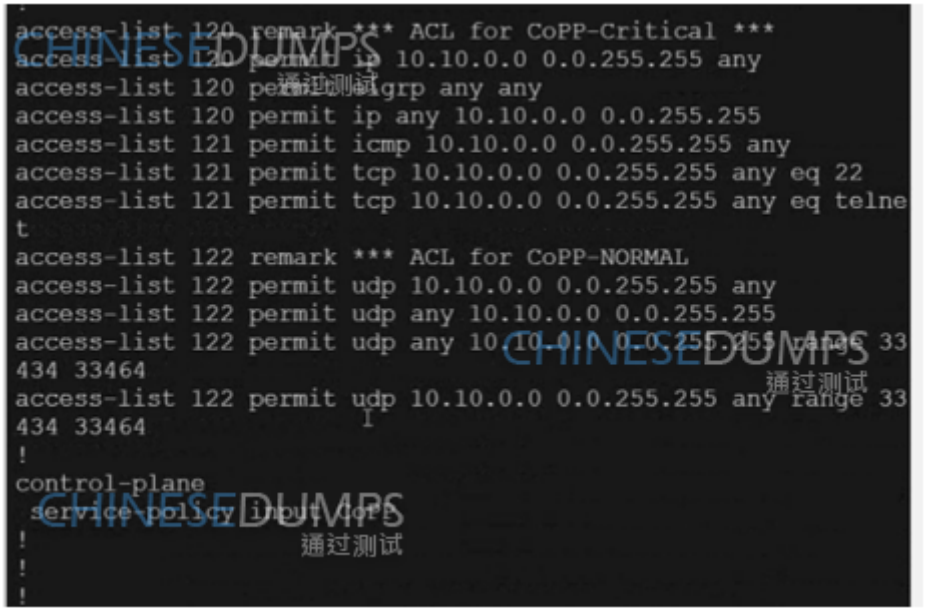
A) Explanation:

CORE

policy-mao CoPP

class CoPP-CRITICAL

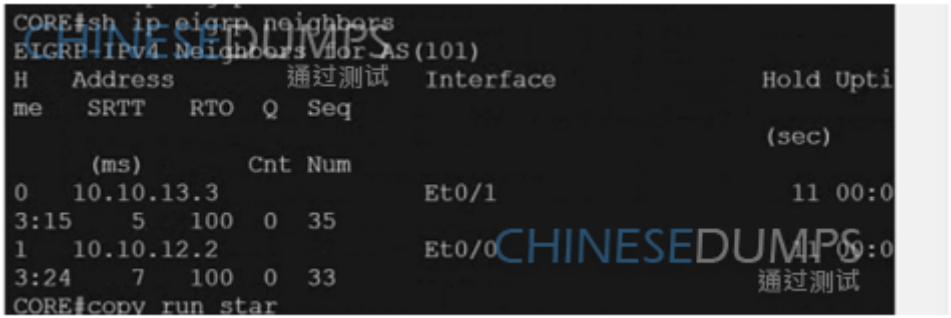
police 1000000 50000 50000 conform-action transmit exceed-action transmit



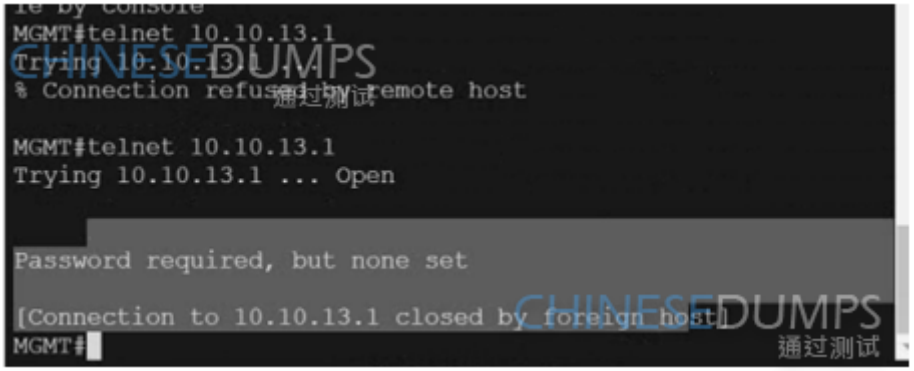
CORE# Copy run start

TESTING: -

CORE



MGMT



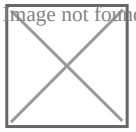
Answer:

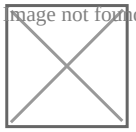
A

Question 10

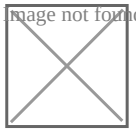
Question Type: **MultipleChoice**

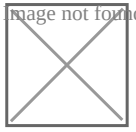
Configure individual VRFs for each customer according to the topology to achieve these goals :

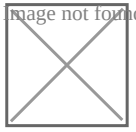


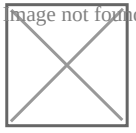


R1









R2

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

SW1

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

SW2

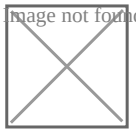


Image not found or type unknown

Image not found or type unknown

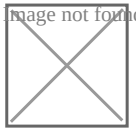


Image not found or type unknown

SW3

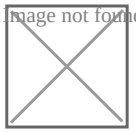


Image not found or type unknown

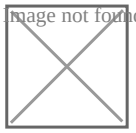


Image not found or type unknown

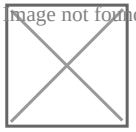


Image not found or type unknown

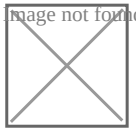


Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Options:

A) Explanation:

Solution:

Use cu-red under interfaces facing SW1 & SW3:

On R1:

interface Ethernet0/0

ip vrf forwarding cu-red

ip address 192.168.1.254 255.255.255.0

Check reachability to SW1:

R1#ping vrf cu-red 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R2:
interface Ethernet0/0
ip vrf forwarding cu-red
ip address 192.168.2.254 255.255.255.0
Check reachability to SW3:
R2#ping vrf cu-red 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Use vrf cu-green for SW2 & SW4:
On R1:
interface Ethernet0/1
ip vrf forwarding cu-green
ip address 192.168.20.254 255.255.255.0
Test reachability to SW2:
R1#ping vrf cu-green 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R2:
interface Ethernet0/1
ip vrf forwarding cu-green
ip address 192.168.22.254 255.255.255.0
Test reachability to SW4:

R2#ping vrf cu-green 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R1:
interface Ethernet0/2.100
mpls ip
!
interface Ethernet0/2.200
mpls ip
!
Configure BGP:
router bgp 65000
neighbor 10.10.10.2 remote-as 65000
neighbor 10.10.20.2 remote-as 65000
!
address-family vpnv4
neighbor 10.10.10.2 activate
neighbor 10.10.20.2 activate
exit-address-family
!
address-family ipv4 vrf cu-green
redistribute connected
exit-address-family
!

address-family ipv4 vrf cu-red
redistribute connected
exit-address-family
!
R1(config)#ip vrf cu-red
R1(config-vrf)#route-target both 65000:100
!
R1(config)#ip vrf cu-green
R1(config-vrf)#route-target both 65000:200
On R2:
interface Ethernet0/2.100
mpls ip
!
interface Ethernet0/2.200
mpls ip
!
router bgp 65000
neighbor 10.10.10.1 remote-as 65000
neighbor 10.10.20.1 remote-as 65000
!
address-family vpnv4
neighbor 10.10.10.1 activate
neighbor 10.10.20.1 activate
exit-address-family
!
address-family ipv4 vrf cu-green

redistribute connected
exit-address-family
!
address-family ipv4 vrf cu-red
redistribute connected
exit-address-family
R2(config)#ip vrf cu-red
R2(config-vrf)#route-target both 65000:100
!
R2(config)#ip vrf cu-green
R2(config-vrf)#route-target both 65000:200
Verification:
From SW1 to SW3:
SW1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW2 or SW4 in VRF cu-green:
SW1#ping 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:

U) U.U
Success rate is 0 percent (0/5)
SW1#ping 192.168.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:

U) U.U
Success rate is 0 percent (0/5)
Same Test for SW2:
From SW2 to SW4:
SW2#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW3 or SW1 in VRF cu-red:
SW2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

U) U.U
Success rate is 0 percent (0/5)
SW2#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

U) U.U
Success rate is 0 percent (0/5)
Both R1 & R2 has separate tables for VRFs cu-red and cu-green.

Answer:

A

To Get Premium Files for 300-410 Visit

https://www.p2pexams.com/products/300-410

For More Free Questions Visit

https://www.p2pexams.com/cisco/pdf/300-410