300-410Q&As

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) (Include 2023 Newest Simulation Labs)

Pass Cisco 300-410 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/300-410.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which command enables NAT-PT on an IPv6 interface?

A. IPv6 nat-pt enable

B. ipv6 nat

C. ipv6 nat-pt

D. ipv6 nat enable

Correct Answer: B

QUESTION 2

Company A recently acquired Company B and the network infrastructures are being merged. Both organizations used non-overlapping globally unique network addressing but different Interior Gateway Protocols (IGPs). Initially, multiple WAN links will connect the two organizations. Company A will maintain its core routing protocol, and Company B\\'s routing protocol will be the edge routing protocol. Two-way redistribution will be used to ensure full network routing capability.

What additional routing configuration should be performed to prevent routing loops and suboptimal routing?

A. Manually configure static routes.

B. Manually configure default routes.

C. Manually adjust the administrative distances.

D. Manually adjust the local preference attribute.

Correct Answer: C

When routes are being redistributed from the core into the edge and from the edge into the core, the administrative distance (AD) associated with external routes should be modified. This lessens the possibility of sub-optimal routing when

multiple routing protocols advertise different paths to the same network. The AD associated with the externally advertised routes should be higher than the internal IGP\\'s AD. To change the AD for an entire routing protocol, use the distance

command. An example and the command syntax are shown below:

router(config)#router rip

router(config-router)#distance 125

The complete syntax of the distance command is:

distance weight [address mask [access-list-number | name]

The weight parameter is the AD, which can be a number from 10 to 255. Note that distances 0 through 9 are reserved

for system use.

To change only the AD for selected networks, use an access list with the distance command as shown below:

router(config)# access-list 5 permit 10.0.0.0 255.0.0.0

router(config)# access-list 5 permit 11.0.0.0 255.0.0.0

router(config)# access-list 5 permit 12.0.0.0 255.0.0.0

router(config)# router rip

router(config-router)# distance 220 0.0.0.0 255.255.255.255 5

The 0.0.0.0 255.255.255.255 portion included with the distance command could hold an address/mask combination for a single address, but it is more common to use an access list.

Objective:

Layer 3 Technologies

Sub-Objective:

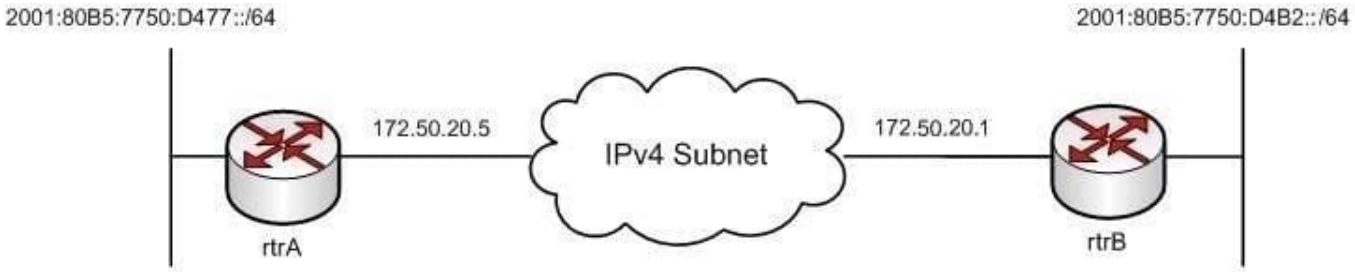
Configure and verify redistribution between any routing protocols or routing sources

References:

Cisco > Cisco IOS IP Routing: Protocol-Independent Command Reference > distance (ip) Cisco > Support > Technology Support > IP > IP Routing > Design > Design Technotes > What Is Administrative Distance? > Document ID: 26634

QUESTION 3

You have implemented an automatic 6-to-4 tunnel between the routers rtrA and rtrB as shown in the following network diagram:



The routers rtrA and rtrB are connected to two IPv6 subnets and are separated by an IPv4 network. You decide to verify whether the tunnel was correctly implemented using the show running-config command. Which of the following commands should exist in the output of the show running-config command on rtrA and rtrB? (Choose all that apply.)

A. interface tunnel

B. tunnel source

C. tunnel destination

D. tunnel mode ipv6ip

E. tunnel mode ipv6ip 6to4

Correct Answer: ABE

The following commands should exist in the output of the show running-config command on rtrA and rtrB: interface tunnel tunnel source

tunnel mode ipv6ip 6to4

The interface tunnel command is used to define a tunnel interface on the router. The tunnel source command allows you to specify the source of the tunnel, which is the router interface that faces the IPv4 network. The tunnel source must be

configured with an IPv4 address. The tunnel mode ipv6ip 6to4 command is used to specify the tunneling mechanism, which in this case is automatic 6-to-4.

The partial output of the show running-config command on rtrA is as follows:

!

interface Tunnel0

no ip address

tunnel mode ipv6ip 6to4

tunnel source 172.50.20.5

ipv6 address 2002:ac32:of06::1/48

!

The partial output of the show running-config command on rtrB is as follows:

!

interface Tunnel0

no ip address

tunnel mode ipv6ip 6to4

tunnel source 172.50.20.1

ipv6 address 2002:ac32:0f06::2/48

!

The tunnel destination command and the tunnel mode ipv6ip commands do not appear in the show running- config output when automatic 6-to-4 tunnels are implemented on rtrA and rtrB. Both of these commands are executed for manually

configured tunnels.

Objective:

Network Principles

Sub-Objective:

Recognize proposed changes to the network

References:

Cisco Press > Articles > Cisco Certification > CCNP > CCNP Self-Study: Advanced IP Addressing Cisco Interface and Hardware Component Configuration Guide > IPv6 Automatic 6to4 Tunnels Cisco > Support > Technology Support > IP >

IP Version 6 (IPV6) > Configure > Configuration Examples and Technotes > IPv6 Tunnel Through an IPv4 Network

Cisco IOS IPv6 Implementation Guide > Implementing Tunneling for IPv6

QUESTION 4

Refer to the Exhibit. A network administrator enables DHCP snooping on the Cisco Catalyst 3750-X switch and configures the uplink port (Port-channel2) as a trusted port. Clients are not receiving an IP address, but when DHCP snooping is disabled, clients start receiving IP addresses.

```
Jan 9 15:29:29.713: DHCP_SNOOPING: process new DHCP packet, message type: DHCPINFORM, input interface:
Po2, MAC da: ffff.ffff.ffff, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0
Jan 9 15:29:29.713: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is
flooded to ingress VLAN: (1)
Jan 9 15:29:29.722: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Vl1 for pak. Was Po2
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1Jan 9
15:29:31.517: DHCP_SNOOPING: received new DHCP packet from input interface (Port-channel2)
```

Which global command resolves the issue?

A. No ip dhcp snooping information option

B. ip dhcp snooping

C. ip dhcp relay information trust portchannel2

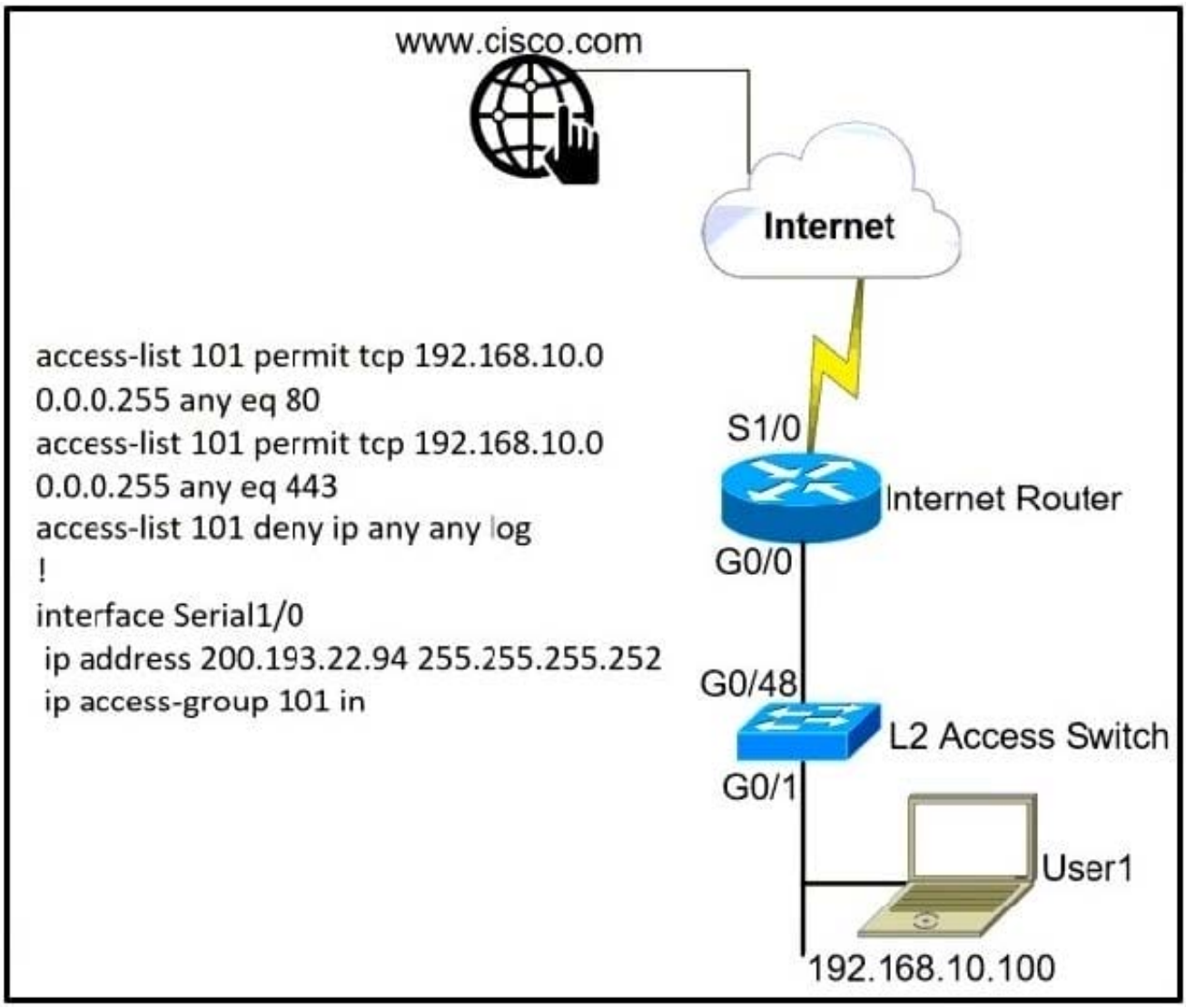
D. ip dhcp snooping trust

Correct Answer: A

https://community.cisco.com/t5/switching/dhcp-snooping-clients-not-getting-ip-address/td-p/1749969

QUESTION 5

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 outgoing direction.

C. Interface S1/0 in the outgoing direction.

D. Interface G0/0 in the incoming direction.

Correct Answer: D