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.leads4pass.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

You want to change the Administrative Distance of external EIGRP routes from the default of 170 to 130 instead on router R1 while leaving the default AD value for internal EIGRP routes. Which set of command will accomplish this?

A. R1(config)#router eigrp R1(config-router)#distance 170

B. R1(config)#router eigrp 1 R1(config-router)#distance eigrp 90 130

C. R1(config)#router eigrp 1 R1(config-router)#distance eigrp 130 90

D. R1(config)#router eigrp 1 R1(config-router)#distance 90 130

Correct Answer: B

QUESTION 2

Which of the following are valid fields in an MPLS header? (Choose four.)

A. Label

B. Sequence Number

C. Experimental (Exp)

D. Bottom of Stack (BoS)

E. Time to Live (TTL)

F. Checksum

Correct Answer: ACDE

QUESTION 3

An administrator attempts to download the pack NBAR2 file using TFTP from the CPE router to another device over the Gi0/0 interface. The CPE is configured as below:

```
hostname CPE
!
ip access-list extended WAN
< >
remark => All UDP rules below for WAN ID: S420T92E35F99
permit udp any eq domain any
permit udp any any eq tftp
deny udp any any
!
interface GigabitEthernet0/0
<...>
ip access-group WAN in
<...>
!
tftp-server flash:pp-adv-csr1000v-1612.1a-37-53.0.0.pack
```

The transfer fails. Which action resolves the issue?

A. Change the WAN ACL to permit the UDP port 69 to allow TFTP

B. Make the permit udp any eq tftp any entry the last entry in the WAN ACL.

C. Change the WAN ACL to permit the entire UDP destination port range

D. Shorten the file name to the 8+3 naming convention.

Correct Answer: B

QUESTION 4

Out of the below options regarding DMVPN and FLEXVPN, select the correct one.

A. FlexVPN uses a new key management protocol ?IKEv2, while most traditional DMVPN networks use IKEv1

B. FlexVPN uses a new key management protocol ?IKEv1, while most traditional DMVPN networks use IKEv2

C. With FlexVPN there\\'s multiple standard way of NHRP and routing protocols operations as opposed to 1 phase of DMVPN

D. Flex VPN and DMVPN both are supported only on Firewalls.

Correct Answer: A

QUESTION 5

An engineer configured VRF-Lite on a router for VRF blue and VRF red. OSPF must be enabled on each VRF to peer to a directly connected router in each VRF. Which configuration forms OSPF neighbors over the network 10.10.10.0/28 for VRF blue and 192.168.0.0/30 for VRF red?

A. router ospf 1 vrf blue network 10.10.10.0 0.0.0.252 area 0 router ospf 2 vrf red network 192.168.0.0 0.0.0.240 area 0

B. router ospf 1 vrf blue network 10.10.10.0 0.0.0.15 area 0 router ospf 2 vrf red network 192.168.0.0 0.0.0.3 area 0

C. router ospf 1 vrf blue network 10.10.10.0 0.0.0.240 area 0 router ospf 2 vrf red network 192.168.0.0 0.0.0.252 area 0

D. router ospf 1 vrf blue network 10.10.10.0 0.0.0.3 area 0 router ospf 2 vrf red network 192 168.0.0 0.0.0.15 are 0

Correct Answer: B

QUESTION 6

What would be a use case for the HSRP configuration below?

```
interface Loopback0
ip address 171.16.6.25

interface Ethernet0
ip address 171.16.6.6 255.255.255.0

no ip redirects
standby 1 ip 171.16.6.100


standby 1 preempt

standby 1 track Loopback0.

interface Serial1
ip address 171.16.7.6 255.255.255.0
```

A. used to switch the active role to the other router in the HSRP group during a maintenance window

B. used to prevent this router from ever relinquishing the active role

C. used to prevent this router from ever performing the active role

D. used to allow preemption over multiple peers

Correct Answer: A

By tracking the loopback interface and decrementing the priority if it goes down, technicians would have a method of moving the active role to the other router by disabling the loopback interface. This method is less disruptive than disabling

any of the physical interfaces. Although no decrement value has been specified, a default decrement of 10 will occur.

This configuration would not be used to prevent this router from ever relinquishing the active role. That would defeat the purpose of Hot Standby Routing Protocol (HSRP), which is to provide failover by relinquishing the active role to the other

router.

This configuration would not be used to prevent this router from ever performing the active role. That would defeat the purpose of HSRP which is to provide failover by this router taking the active role when there is an issue with the other

router.

This configuration would not be used to allow preemption over multiple peers. When more than two routers are in an HSRP group, the active router is allowed preemption over multiple peers by default.

Objective:

Infrastructure Services

Sub-Objective:

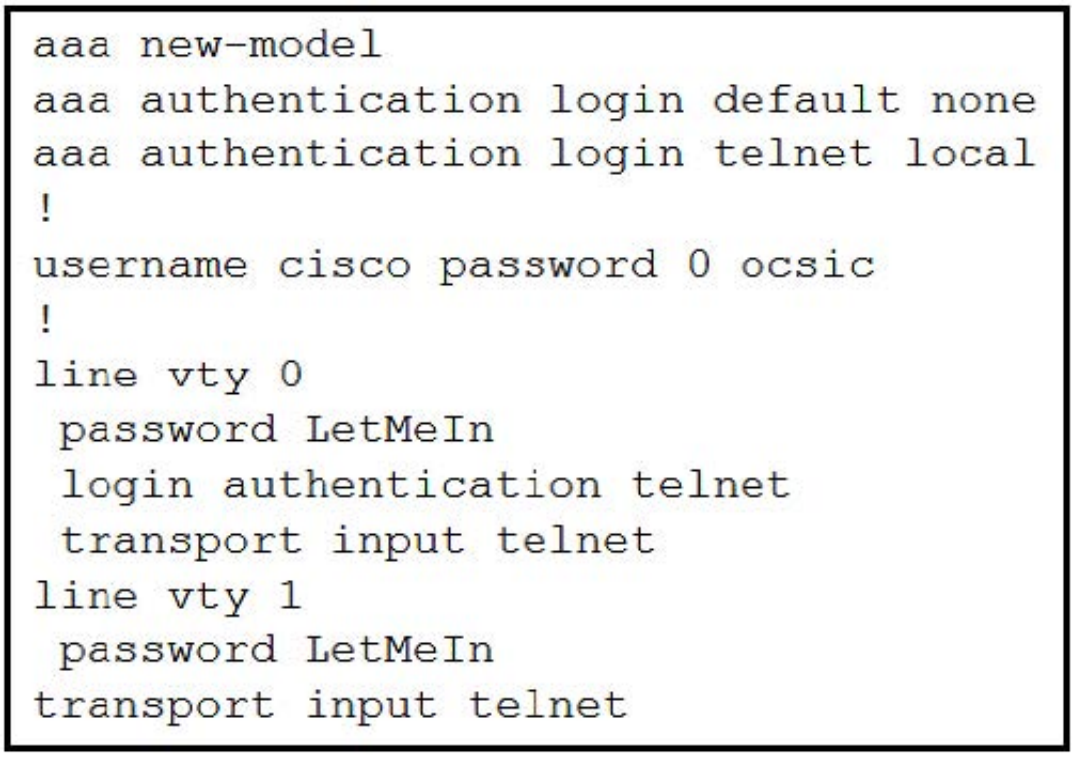
Configure and verify tracking objects

References:

Home > Support > Technology support > IP > IP application services > Troubleshoot and alerts > Troubleshooting Technotes > How to use the standby preempt and standby track commands

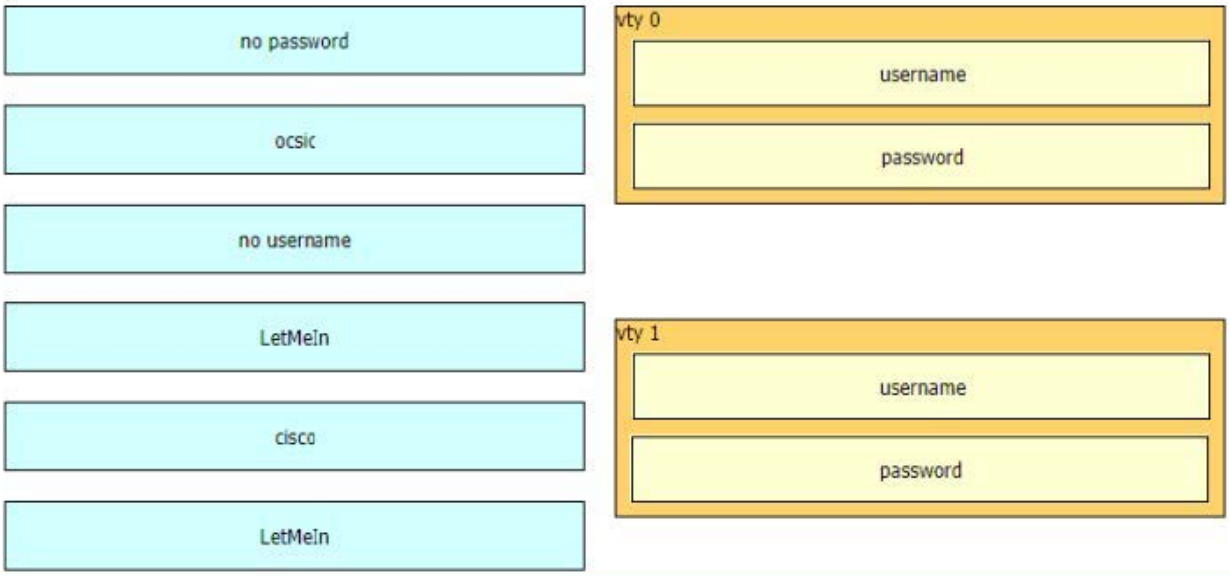
QUESTION 7

DRAG DROP Refer to the exhibit.



Drag and drop the credentials from the left onto the remote login information on the right to resolve a failed login attempt to vtys. Not all credentials are used.

Select and Place:



Correct Answer:

vty 0:

+

cisco

+

0csic

vty 1:

+

no username

+

no password

The command “aaa authentication login default none” means no authentication is required when access to the device via Console/VTY/AUX so if one interface does not specify another login authentication method (via the “login authentication …” command), it will allow to access without requiring username or password. In this case VTY 1 does not specify another authentication login method so it will use the default method (which is “none” in this case).

QUESTION 8

Which configuration feature should be used to block rogue router advertisements instead of using the IPv6 Router Advertisement Guard feature?

A. VACL blocking broadcast frames from nonauthorized hosts

B. IPv4 ACL blocking route advertisements from nonauthorized hosts

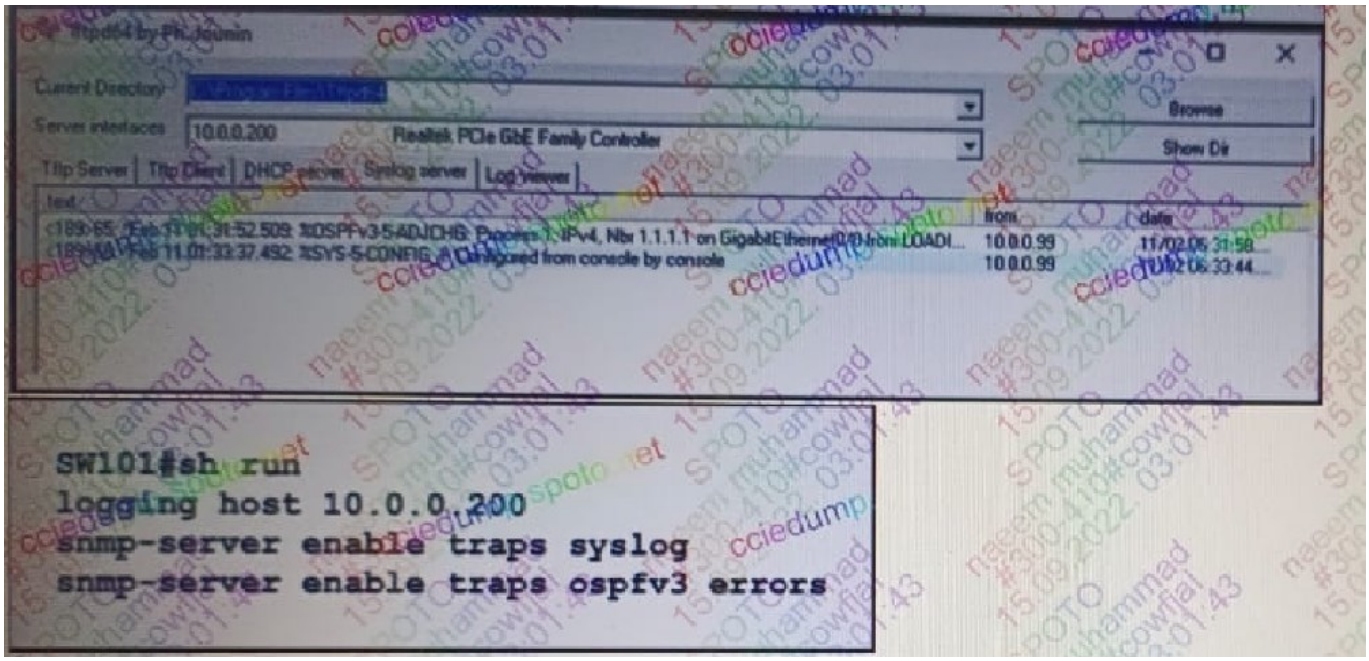
C. PVLANs with promiscuous ports associated to route advertisements and isolated ports for nodes

D. PVLANs with community ports associated to route advertisements and isolated ports for nodes

Correct Answer: C

QUESTION 9

Refer to the exhibit.



An engineer configures SW101 to send OSPFv3 interfaces state change messages to the server. However, only some

OSPFv3 errors are being recorded. Which organization resolves the ..?

A. snmp-server enable traps ospfv3 state-change if-state-change

B. snmp-server-enable traps ospfv3 state-change restart-status-change

C. snmp-server-enable traps ospfv3 state-change neighbor-state-change.

D. snmp-server-enable traps ospfv3 state-change if-state-change neighbor-state-change

Correct Answer: D

QUESTION 10

You just discovered that a ping packet sent from one of the devices to another took a different path in the return than it did on its way to the destination.

What behavior caused this?

A. Windowing

B. Global synchronization

C. MSS

D. Asymmetric routing

Correct Answer: D

This behavior is caused by asymmetric routing. This is quite common in a routed network and usually is not a problem. It can, however, become an issue when firewalls reside in a routed path. Firewalls can cause problems when they

maintain state information about connections. State information is used to determine if return connection is allowed. If the return path is routed through a different firewall, it will not have the correct state information for the connection, and the

return will be disallowed.

It is not caused by windowing. This is a technique used to adjust the number of packets that can be acknowledged at once by a receiving computer in a transmission. In times of congestion, the window or number of packets that can be

acknowledged at a time will be small. Later, when congestion goes down, the window size can be increased.

The behavior is not caused by the maximum segment size (MSS). This value specifies the largest amount of data, in octets, that a computer or communications device can receive in a single TCP segment. This will not cause a packet to take

a different path in the return than it did on its way to the destination.

The behavior is not caused by global synchronization. This occurs when congestion on the network causes all devices to reduce their transmission rates at the same time. The result is the network cycling between sharp increases and sharp

decreases in traffic.

Objective:

Network Principles

Sub-Objective:

Explain TCP operations

References:

Home > Services > Technical services newsletter > Tech insights > Chalk talk > Asymmetric Routing and Firewalls

QUESTION 11

What is an advantage of using BFD?

A. It detects local link failure at layer 1 and updates routing table.

B. It detects local link failure at layer 2 and updates routing protocols.

C. It has sub-second failure detection for layer 1 and layer 3 problems.

D. It has sub-second failure detection for layer 1 and layer 2 problems.

Correct Answer: C

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels

QUESTION 12

What are two functions of MPLS Layer 3 VPNs? (Choose two.)

A. LDP and BGP can be used for Pseudowire signaling.

B. It is used for transparent point-to-multipoint connectivity between Ethernet links/sites.

C. BGP is used for signaling customer VPNv4 routes between PE nodes.

D. A packet with node segment ID is forwarded along with shortest path to destination.

E. Customer traffic is encapsulated in a VPN label when it is forwarded in MPLS network.

Correct Answer: CE

MPLS Layer-3 VPNs provide IP connectivity among CE sites

*

MPLS VPNs enable full-mesh, hub-andspoke, and hybrid IP connectivity

*

CE sites connect to the MPLS network via IP peering across PE-CE links

*

MPLS Layer-3 VPNs are implemented via VRFs on PE edge nodes

*

VRFs providing customer routing and forwarding segmentation

*

BGP used for signaling customer VPN (VPNv4) routes between PE nodes

*

To ensure traffic separation, customer traffic is encapsulated in an additional VPN label when forwarded in MPLS network

*

Key applications are layer-3 business VPN services, enterprise network segmentation, and segmented layer-3 Data Center access

---

QUESTION 13

An engineer configures PBR en R5 and wants to create a policy that matches traffic destined foward 10.10.10.0/24 and forwards it toward 10.1.1 1. This traffic must also have its IP precedence set to 5. All other traffic should be forwarded toward 10.1.1.2 and have its IP precedence set to 0.

Which configuration meets the requirements?

A. access-list 1 permit 10.10.10.0 0.0.0.255 access-list 2 permit any route-map CCNP permit 10 match ip address 1 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 match ip address 2 set ip next-hop 10.1.1.2 set ip precedence 0route-map CCNP permit 30

B. access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 100 set ip next-hop 10.1.1.1 set ip precedence 0 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 5 ! route-map CCNP permit 30

C. access-list 1 permit 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 1 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 0

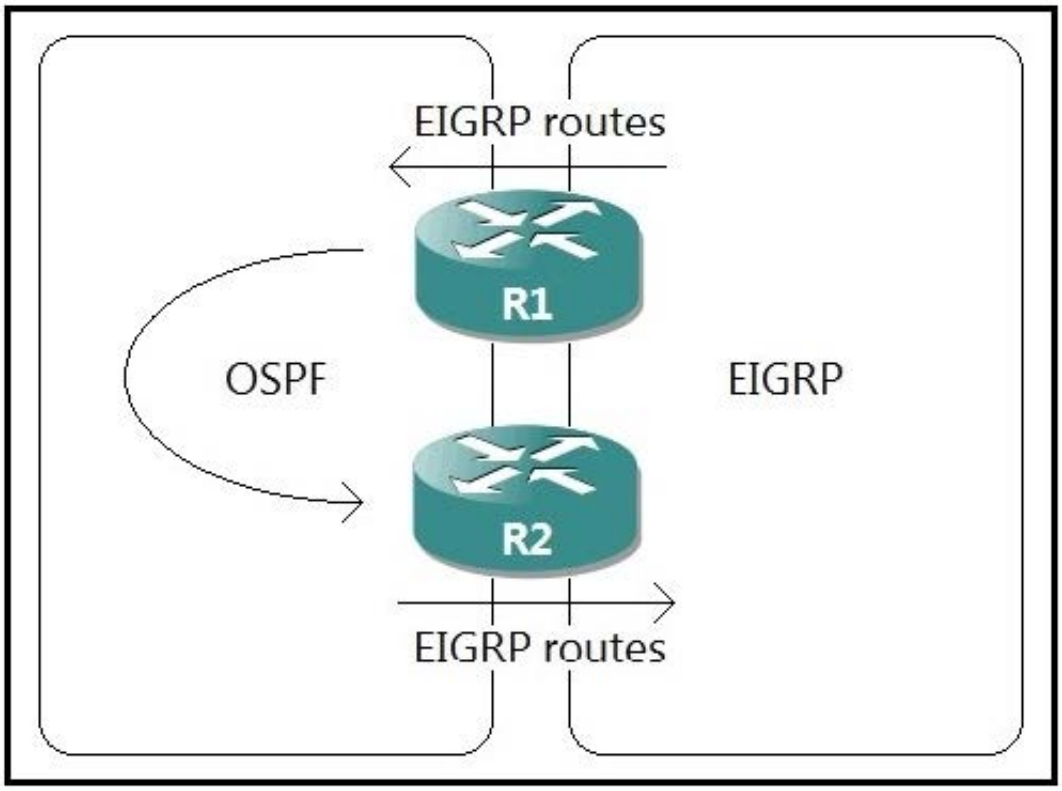
D. access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 100 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 0

Correct Answer: D

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/pbroute.pdf
Classify traffic based on extended access list criteria.

QUESTION 14

Refer to the exhibit. A network administrator configured mutual redistribution on R1 and R2 routers, which caused instability in the network.



Which action resolves the issue?

A. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to deny when redistributing OSPF into EIGRP.

B. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to allow when redistributing OSPF into EIGRP.

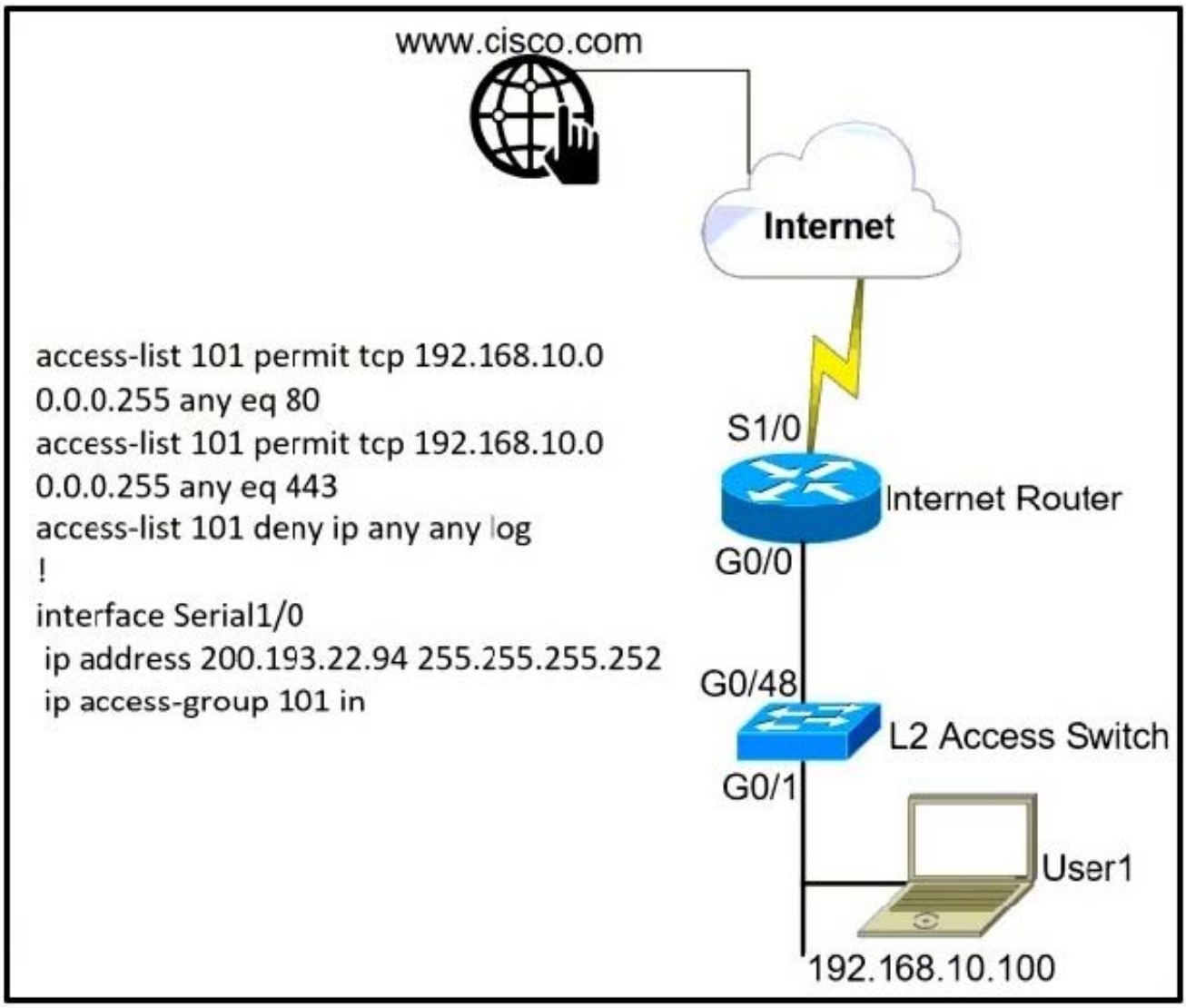
C. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.

D. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.

Correct Answer: A

QUESTION 15

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