CCNA 200-125

Cisco Certified Network Associate (CCNA v3.0)

Thank You for Downloading 200-125 Updated Exam Questions

https://www.theexamcerts.com/cisco/200-125-pdf-exam-dumps

Version: 13.0

Question: 1

Refer to the exhibit:

Router1# **show ip arp**

Protocol	Address	Age(min)	Hardware Adddr	Type	Interface
Internet	192.168.20.5	9	0000.0c07.f892	ARPA	FastEthernet0/0
Internet	192.168.60.5	8	0000.0c07.ac00	ARPA	FastEthernet0/1
Internet	192.168.20.1	-	0000.0c63.ae45	ARPA	FastEthernet0/0
Internet	192.168.40.5	9	0000.0c07.4320	ARPA	FastEthernet0/2
Internet	192.168.60.1	-	0000.0c63.1300	ARPA	FastEthernet0/1
Internet	192.168.40.1	-	0000.0c36.6965	ARPA	FastEthernet0/2

Data Frame:

Source MAC	Source IP	Destination MAC	Destination IP
0000.0c07.f892	192.168.20.5	0000.0c63.ae45	192.168.40.5

What will Router1 do when it receives the data frame shown? (Choose three.)

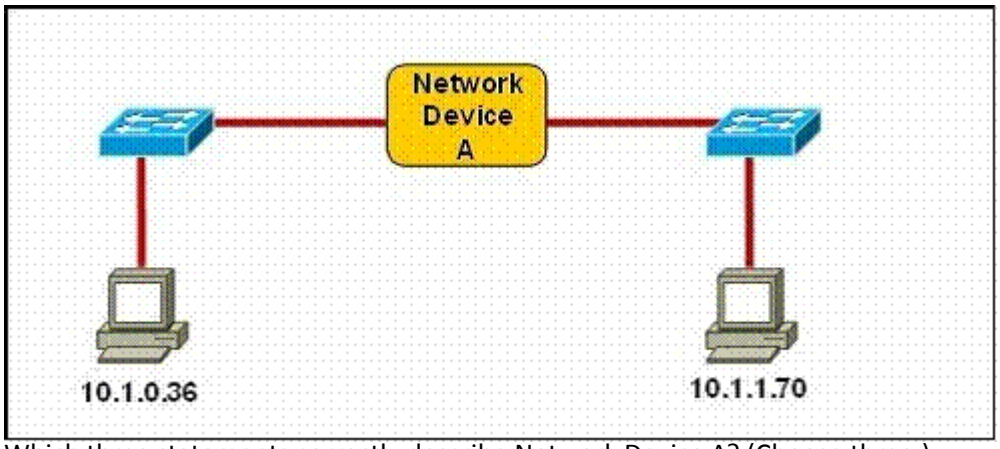
A. Router1 will strip off the source MAC address and replace it with the MAC address 0000.0c36.6965.
B. Router1 will strip off the source IP address and replace it with the IP address 192.168.40.1.
C. Router1 will strip off the destination MAC address and replace it with the MAC address 0000.0c07.4320.
D. Router1 will strip off the destination IP address and replace it with the IP address of 192.168.40.1.
E. Router1 will forward the data packet out interface FastEthernet0/1.
F. Router1 will forward the data packet out interface FastEthernet0/2.

Answer: A, C, F

Explanation:
Remember, the source and destination MAC changes as each router hop along with the TTL being decremented but the source and destination IP address remain the same from source to destination.

Question: 2

Refer to the exhibit.



Which three statements correctly describe Network Device A? (Choose three.)

A. With a network wide mask of 255.255.255.128, each interface does not require an IP address.
B. With a network wide mask of 255.255.255.128, each interface does require an IP address on a unique IP subnet.
C. With a network wide mask of 255.255.255.0, must be a Layer 2 device for the PCs to communicate with each other.
D. With a network wide mask of 255.255.255.0, must be a Layer 3 device for the PCs to communicate with each other.
E. With a network wide mask of 255.255.254.0, each interface does not require an IP address.

Answer: B, D, E

Explanation:
If Subnet Mask is 255.255.255.128 the hosts vary from x.x.x.0 - x.x.x.127 & x.x.x.128- x.x.x.255, so the IP Addresses of 2 hosts fall in different subnets so each interface needs an IP an address so that they can communicate each other.
If Subnet Mask is 255.255.255.0 the 2 specified hosts fall in different subnets so they need a Layer 3 device to communicate.
If Subnet Mask is 255.255.254.0 the 2 specified hosts are in same subnet so are in network address and can be accommodated in same Layer 2 domain and can communicate with each other directly using the Layer 2 address.

Question: 3

Which layer in the OSI reference model is responsible for determining the availability of the receiving program and checking to see if enough resources exist for that communication?

A. transport
B. network
C. presentation
D. session
E. application

Answer: E

Explanation:
This question is to examine the OSI reference model.
The Application layer is responsible for identifying and establishing the availability of the intended communication partner and determining whether sufficient resources for the intended communication exist.

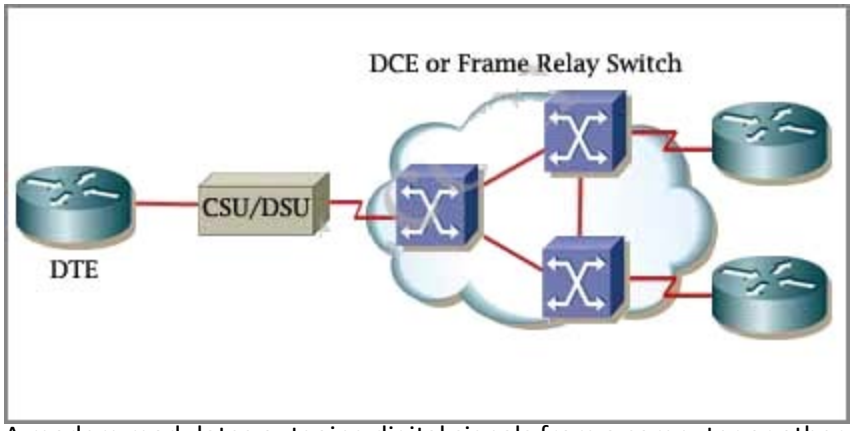
Question: 4

Which of the following describes the roles of devices in a WAN? (Choose three.)

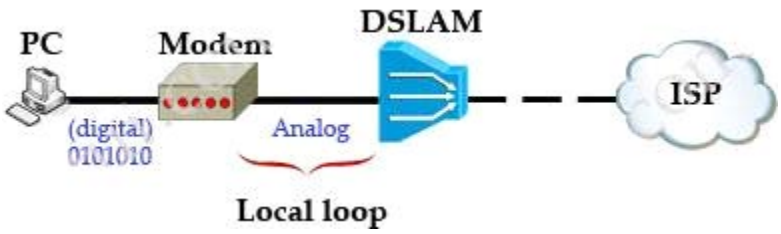
A. A CSU/DSU terminates a digital local loop.
B. A modem terminates a digital local loop.
C. A CSU/DSU terminates an analog local loop.
D. A modem terminates an analog local loop.
E. A router is commonly considered a DTE device.
F. A router is commonly considered a DCE device.

Answer: A, D, E

Explanation:
The idea behind a WAN is to be able to connect two DTE networks together through a DCE network. The network's DCE device (includes CSU/DSU) provides clocking to the DTE-connected interface (the router's serial interface).

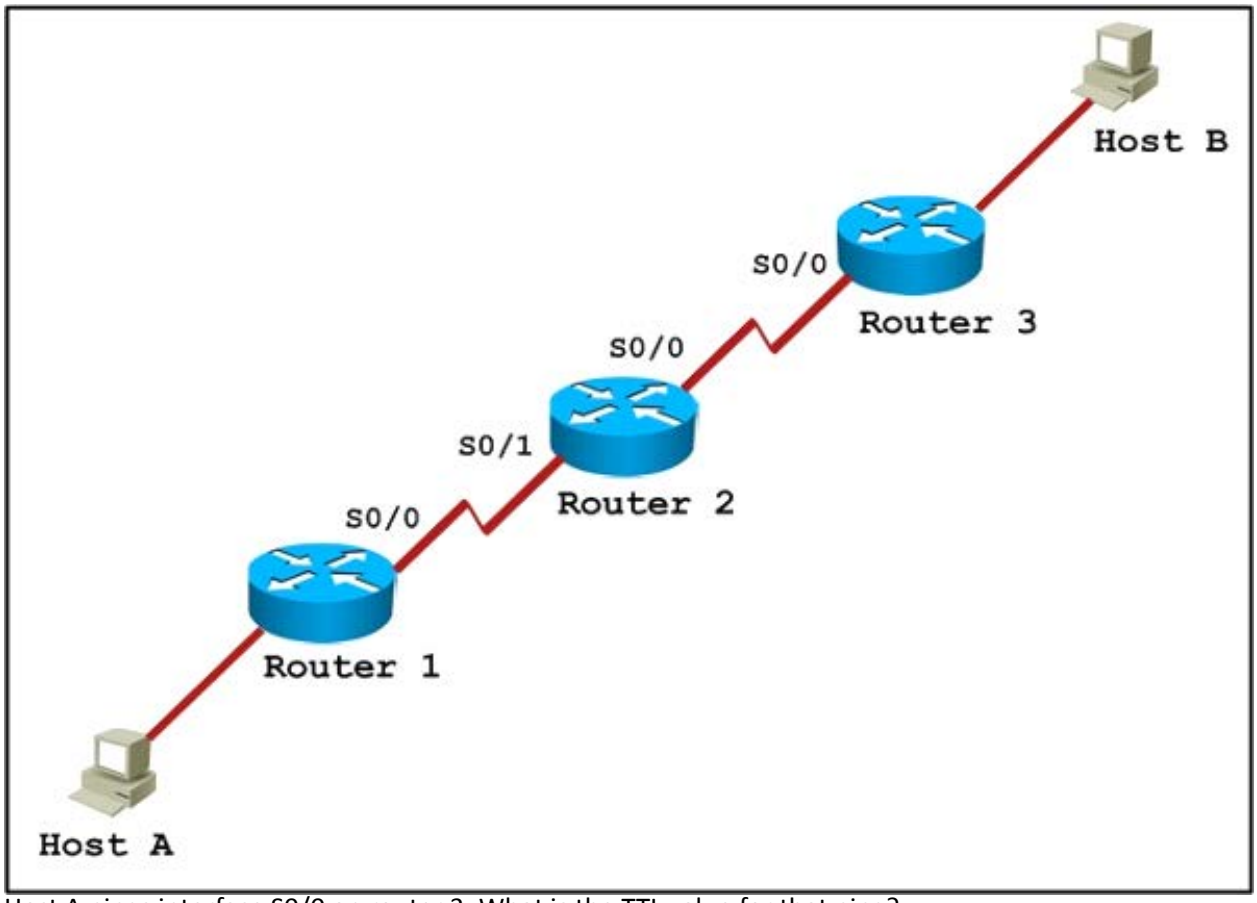


A modem modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device. A CSU/DSU is used between two digital lines -
For more explanation of answer D, in telephony the local loop (also referred to as a subscriber line) is the physical link or circuit that connects from the demarcation point of the customer premises to the edge of the carrier or telecommunications service provider's network. Therefore a modem terminates an analog local loop is correct.



Question: 5

Refer to the exhibit.



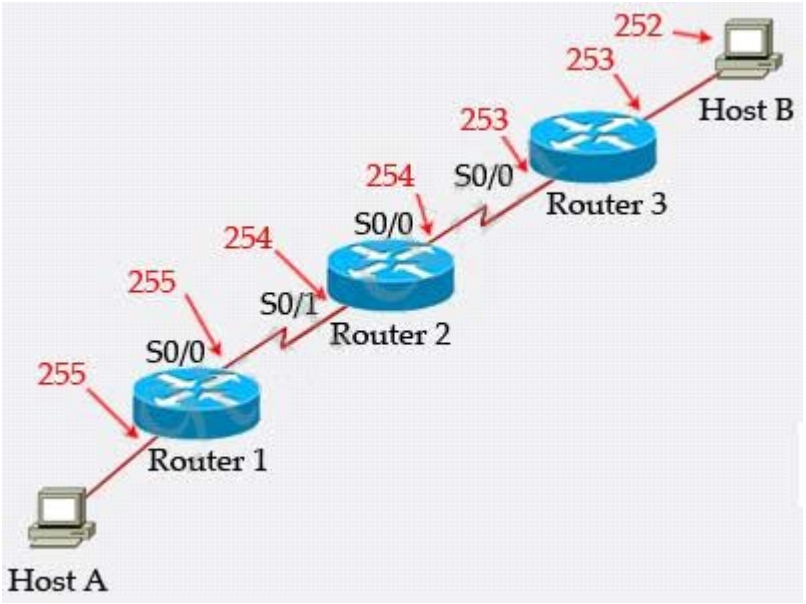
Host A pings interface S0/0 on router 3. What is the TTL value for that ping?

A. 252
B. 253
C. 254
D. 255

Answer: B

Explanation:
From the CCNA ICND2 Exam book: "Routers decrement the TTL by 1 every time they forward a packet; if a router decrements the TTL to 0, it throws away the packet. This prevents packets from

rotating forever." I want to make it clear that before the router forwards a packet, the TTL is still remain the same. For example in the topology above, pings to S0/1 and S0/0 of Router 2 have the same TTL.
The picture below shows TTL values for each interface of each router and for Host B. Notice that Host A initializes ICMP packet with a TTL of 255:



Question: 6

A network administrator is verifying the configuration of a newly installed host by establishing an FTP connection to a remote server. What is the highest layer of the protocol stack that the network administrator is using for this operation?

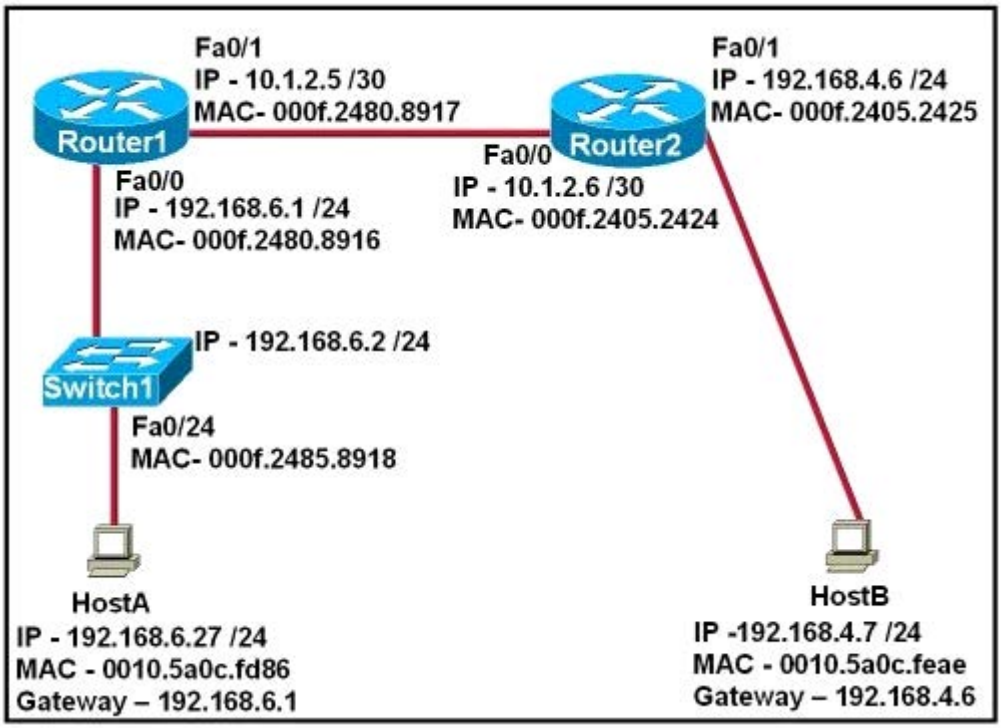
A. application
B. presentation
C. session
D. transport
E. internet
F. data link

Answer: A

Explanation:
FTP belongs to Application layer and it is also the highest layer of the OSI model.

Question: 7

Refer to the exhibit.



After HostA pings HostB, which entry will be in the ARP cache of HostA to support this transmission?

A.

Interface Address	Physical Address	Type
192.168.4.7	000f.2480.8916	dynamic

B.

Interface Address	Physical Address	Type
192.168.4.7	0010.5a0c.feae	dynamic

C.

Interface Address	Physical Address	Type
192.168.6.1	0010.5a0c.feae	dynamic

D.

Interface Address	Physical Address	Type
192.168.6.1	000f.2480.8916	dynamic

E.

Interface Address	Physical Address	Type
192.168.6.2	0010.5a0c.feae	dynamic

F.

Interface Address	Physical Address	Type
192.168.6.2	000f.2485.8918	dynamic

A. Exhibit A
B. Exhibit B
C. Exhibit C
D. Exhibit D
E. Exhibit E
F. Exhibit F

Answer: A

Explanation:
Host A knows host B is in another network so it will send the pings to its default gateway 192.168.6.1. Host A sends a broadcast frame asking the MAC address of 192.168.6.1. This information (IP and MAC address of the default gateway) is saved in its ARP cache for later use.

Question: 8

A network interface port has collision detection and carrier sensing enabled on a shared twisted pair network. From this statement, what is known about the network interface port?

A. This is a 10 Mb/s switch port.
B. This is a 100 Mb/s switch port.
C. This is an Ethernet port operating at half duplex.
D. This is an Ethernet port operating at full duplex.
E. This is a port on a network interface card in a PC.

Answer: C

Explanation:
Modern Ethernet networks built with switches and full-duplex connections no longer utilize CSMA/CD. CSMA/CD is only used in obsolete shared media Ethernet (which uses repeater or hub).

Question: 9

A receiving host computes the checksum on a frame and determines that the frame is damaged. The frame is then discarded. At which OSI layer did this happen?

A. session
B. transport
C. network
D. data link
E. physical

Answer: D

Explanation:
The Data Link layer provides the physical transmission of the data and handles error notification, network topology, and flow control. The Data Link layer formats the message into pieces, each called a data frame, and adds a customized header containing the hardware destination and source address. Protocols Data Unit (PDU) on Datalink layer is called frame. According to this question the frame is damaged and discarded which will happen at the Data Link layer.

Question: 10

Which of the following correctly describe steps in the OSI data encapsulation process? (Choose two.)

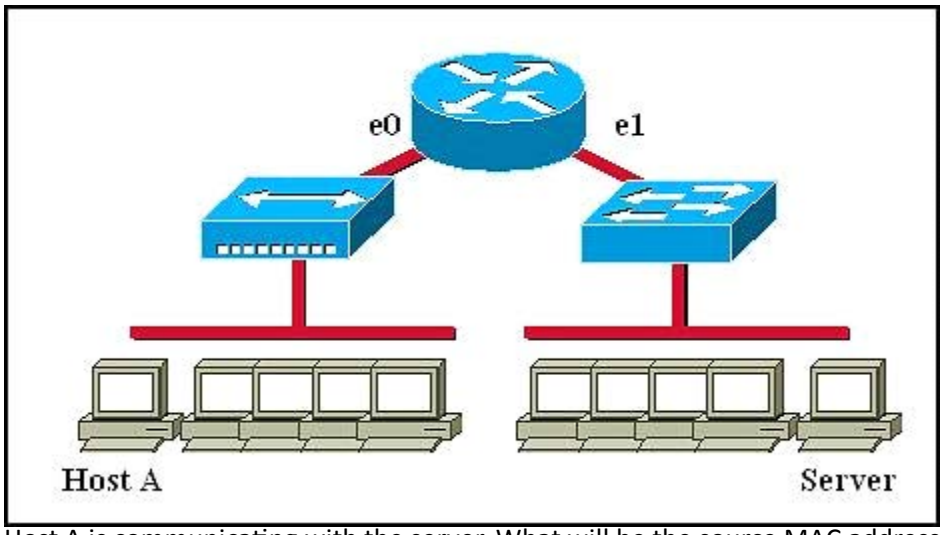
A. The transport layer divides a data stream into segments and may add reliability and flow control information.
B. The data link layer adds physical source and destination addresses and an FCS to the segment.
C. Packets are created when the network layer encapsulates a frame with source and destination host addresses and protocol-related control information.
D. Packets are created when the network layer adds Layer 3 addresses and control information to a segment.
E. The presentation layer translates bits into voltages for transmission across the physical link.

Answer: A, D

Explanation:
The transport layer segments data into smaller pieces for transport. Each segment is assigned a sequence number, so that the receiving device can reassemble the data on arrival.
The transport layer also use flow control to maximize the transfer rate while minimizing the requirements to retransmit. For example, in TCP, basic flow control is implemented by acknowledgment by the receiver of the receipt of data; the sender waits for this acknowledgment before sending the next part.
The Network layer (Layer 3) has two key responsibilities. First, this layer controls the logical addressing of devices. Second, the network layer determines the best path to a particular destination network, and routes the data appropriately.

Question: 11

Refer to the graphic.



Host A is communicating with the server. What will be the source MAC address of the frames received by Host A from the server?

A. the MAC address of router interface e0
B. the MAC address of router interface e1
C. the MAC address of the server network interface

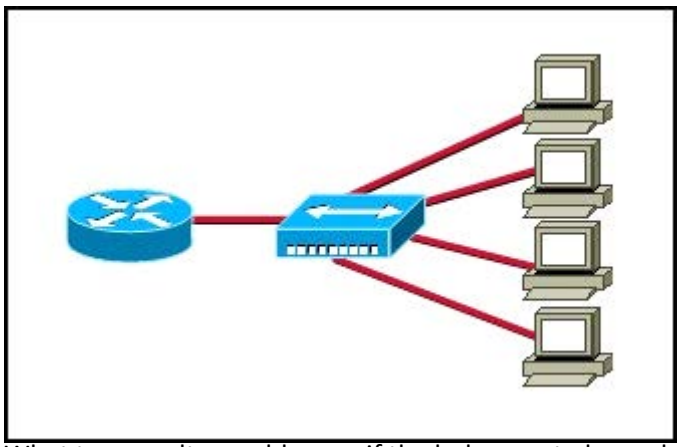
D. the MAC address of host A

Answer: A

Explanation:
Whereas switches can only examine and forward packets based on the contents of the MAC header, routers can look further into the packet to discover the network for which a packet is destined. Routers make forwarding decisions based on the packet's network-layer header (such as an IPX header or IP header). These network-layer headers contain source and destination network addresses. Local devices address packets to the router's MAC address in the MAC header. After receiving the packets, the router must perform the following steps:
1. Check the incoming packet for corruption, and remove the MAC header. The router checks the packet for MAC-layer errors. The router then strips off the MAC header and examines the network-layer header to determine what to do with the packet.
2. Examine the age of the packet. The router must ensure that the packet has not come too far to be forwarded. For example, IPX headers contain a hop count. By default, 15 hops is the maximum number of hops (or routers) that a packet can cross. If a packet has a hop count of 15, the router discards the packet. IP headers contain a Time to Live (TTL) value. Unlike the IPX hop count, which increments as the packet is forwarded through each router, the IP TTL value decrements as the IP packet is forwarded through each router. If an IP packet has a TTL value of 1, the router discards the packet. A router cannot decrement the TTL value to 1 and then forward the packet.
3. Determine the route to the destination. Routers maintain a routing table that lists available networks, the direction to the desired network (the outgoing interface number), and the distance to those networks. After determining which direction to forward the packet, the router must build a new header. (If you want to read the IP routing tables on a Windows 95/98 workstation, type ROUTE PRINT in the DOS box.)
4. Build the new MAC header and forward the packet. Finally, the router builds a new MAC header for the packet. The MAC header includes the router's MAC address and the final destination's MAC address or the MAC address of the next router in the path.

Question: 12

Refer to the exhibit.



What two results would occur if the hub were to be replaced with a switch that is configured with one Ethernet VLAN? (Choose two.)

A. The number of collision domains would remain the same.
B. The number of collision domains would decrease.
C. The number of collision domains would increase.
D. The number of broadcast domains would remain the same.
E. The number of broadcast domains would decrease.
F. The number of broadcast domains would increase.

Answer: C, D

Explanation:
Basically, a collision domain is a network segment that allows normal network traffic to flow back and forth. In the old days of hubs, this meant you had a lot of collisions, and the old CSMA/CD would be working overtime to try to get those packets re-sent every time there was a collision on the wire (since Ethernet allows only one host to be transmitting at once without there being a traffic jam). With switches, you break up collision domains by switching packets bound for other collision domains. These days, since we mostly use switches to connect computers to the network, you generally have one collision domain to a PC.
Broadcast domains are exactly what they imply: they are network segments that allow broadcasts to be sent across them. Since switches and bridges allow for broadcast traffic to go unswitched, broadcasts can traverse collision domains freely. Routers, however, don't allow broadcasts through by default, so when a broadcast hits a router (or the perimeter of a VLAN), it doesn't get forwarded. The simple way to look at it is this way: switches break up collision domains, while routers (and VLANs) break up collision domains and broadcast domains. Also, a broadcast domain can contain multiple collision domains, but a collision domain can never have more than one broadcast domain associated with it.
Collision Domain: A group of Ethernet or Fast Ethernet devices in a CSMA/CD LAN that are connected by repeaters and compete for access on the network. Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network in order to avoid data collisions. A collision domain is sometimes referred to as an Ethernet segment.
Broadcast Domain: Broadcasting sends a message to everyone on the local network (subnet). An example for Broadcasting would be DHCP Request from a Client PC. The Client is asking for a IP Address, but the client does not know how to reach the DHCP Server. So the client sends a DHCP Discover packet to EVERY PC in the local subnet (Broadcast). But only the DHCP Server will answer to the Request.
How to count them?
Broadcast Domain:
No matter how many hosts or devices are connected together, if they are connected with a repeater, hub, switch or bridge, all these devices are in ONE Broadcast domain (assuming a single VLAN). A Router is used to separate Broadcast-Domains (we could also call them Subnets - or call them VLANs).
So, if a router stands between all these devices, we have TWO broadcast domains.
Collision Domain:
Each connection from a single PC to a Layer 2 switch is ONE Collision domain. For example, if 5 PCs are connected with separate cables to a switch, we have 5 Collision domains. If this switch is connected to another switch or a router, we have one collision domain more.
If 5 Devices are connected to a Hub, this is ONE Collision Domain. Each device that is connected to a Layer 1 device (repeater, hub) will reside in ONE single collision domain.

Question: 13

Which three statements accurately describe Layer 2 Ethernet switches? (Choose three.)

A. Spanning Tree Protocol allows switches to automatically share VLAN information.
B. Establishing VLANs increases the number of broadcast domains.
C. Switches that are configured with VLANs make forwarding decisions based on both Layer 2 and Layer 3 address information.
D. Microsegmentation decreases the number of collisions on the network.
E. In a properly functioning network with redundant switched paths, each switched segment will contain one root bridge with all its ports in the forwarding state. All other switches in that broadcast domain will have only one root port.
F. If a switch receives a frame for an unknown destination, it uses ARP to resolve the address.

Answer: B, D, E

Explanation:
Microsegmentation is a network design (functionality) where each workstation or device on a network gets its own dedicated segment (collision domain) to the switch. Each network device gets the full bandwidth of the segment and does not have to share the segment with other devices. Microsegmentation reduces and can even eliminate collisions because each segment is its own collision domain ->.
Note: Microsegmentation decreases the number of collisions but it increases the number of collision domains.

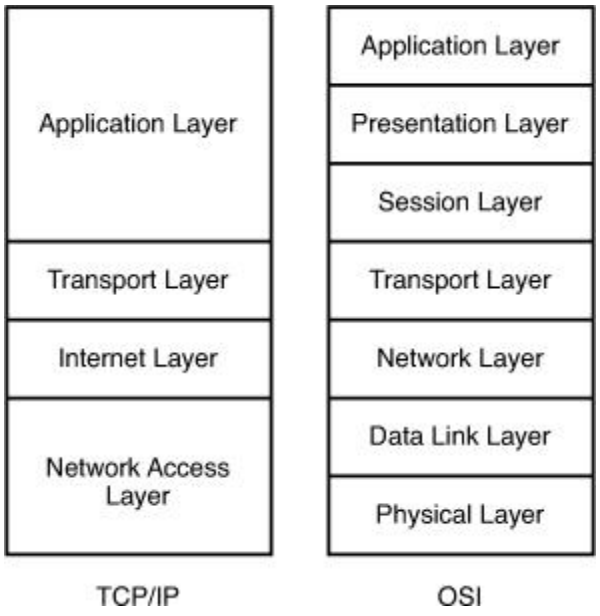
Question: 14

Where does routing occur within the DoD TCP/IP reference model?

A. application
B. internet
C. network
D. transport

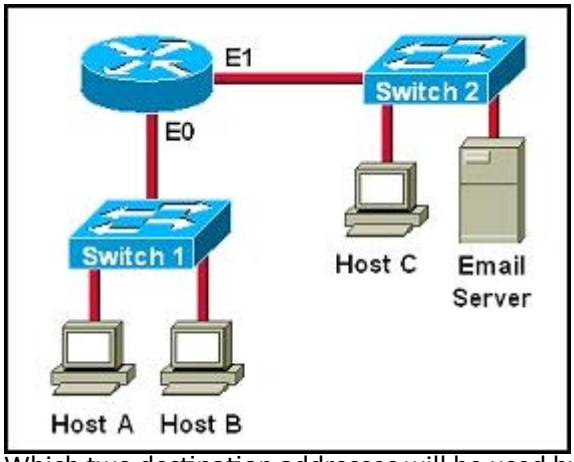
Answer: B

Explanation:
The picture below shows the comparison between TCP/IP model & OSI model. Notice that the Internet Layer of TCP/IP is equivalent to the Network Layer which is responsible for routing decision.



Question: 15

Refer to exhibit:



Which two destination addresses will be used by Host A to send data to Host C? (Choose two.)

A. the IP address of Switch 1
B. the MAC address of Switch 1
C. the IP address of Host C
D. the MAC address of Host C
E. the IP address of the router's E0 interface
F. the MAC address of the router's E0 interface

Answer: C, F

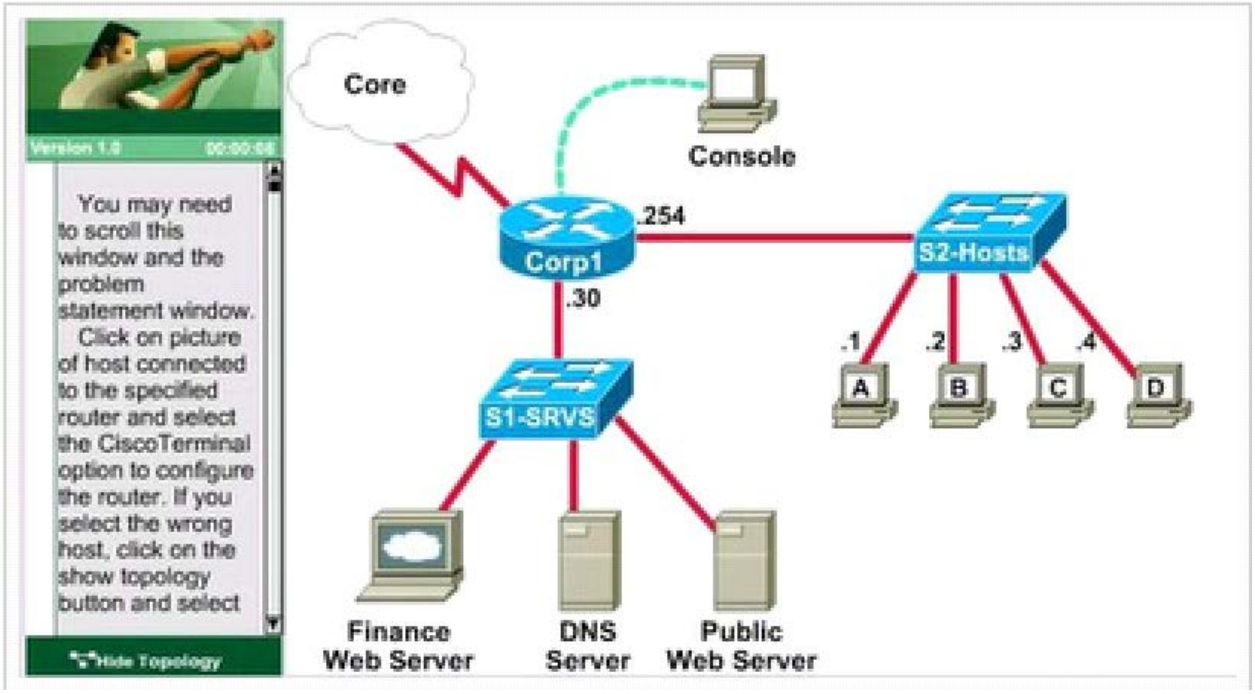
Explanation:
While transferring data through many different networks, the source and destination IP addresses are not changed. Only the source and destination MAC addresses are changed. So in this case Host A

will use the IP address of Host C and the MAC address of E0 interface to send data. When the router receives this data, it replaces the source MAC address with its own E1 interface's MAC address and replaces the destination MAC address with Host C's MAC address before sending to Host C.

Question: 16

SIMULATION

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.
The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.
Access to the router CLI can be gained by clicking on the appropriate host.
All passwords have been temporarily set to "cisco".
The Core connection uses an IP address of 198.18.196.65.
The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254
host A 192.168.33.1
host B 192.168.33.2
host C 192.168.33.3
host D 192.168.33.4
The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30.
The Finance Web Server is assigned an IP address of 172.22.242.23.

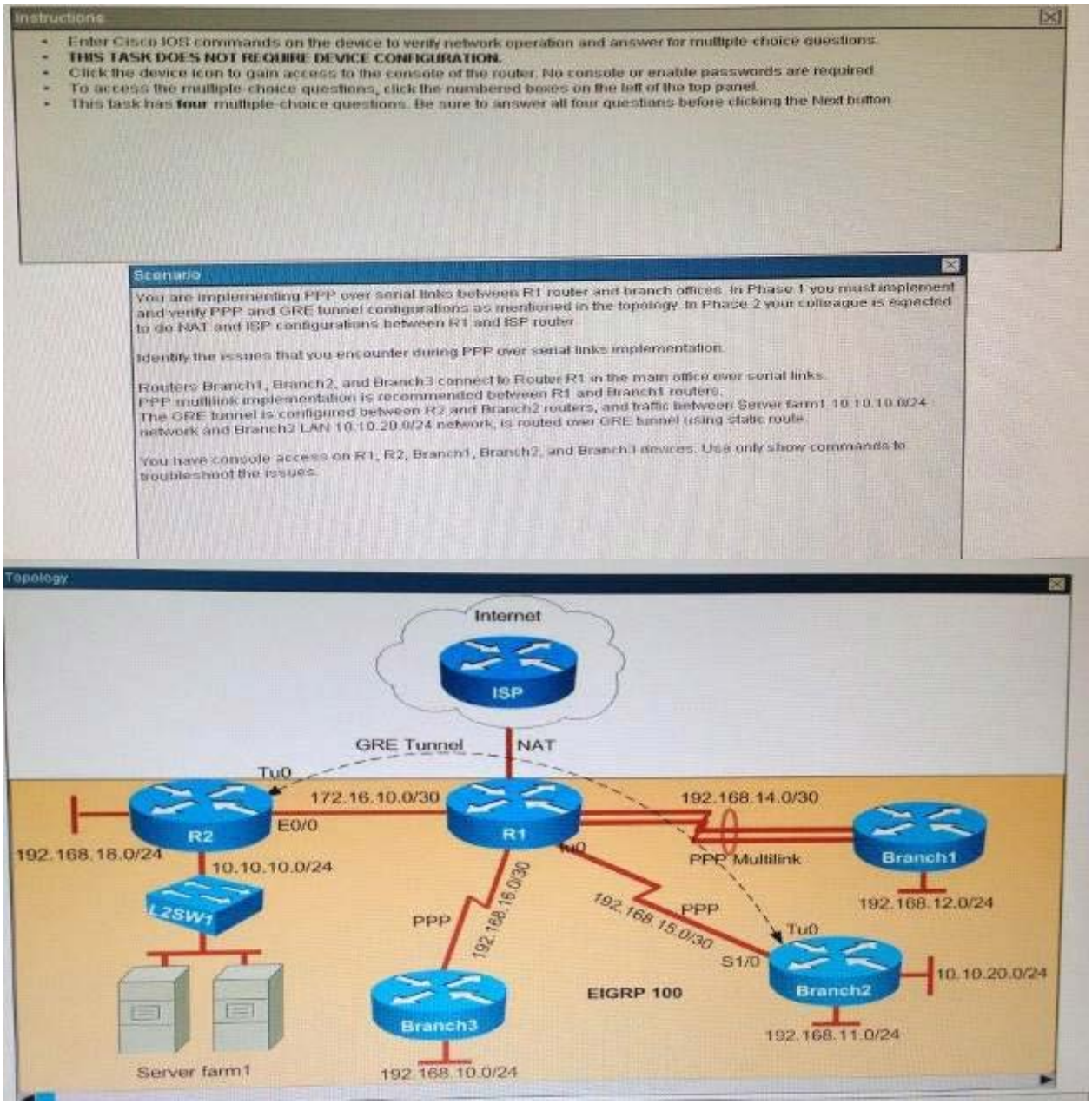


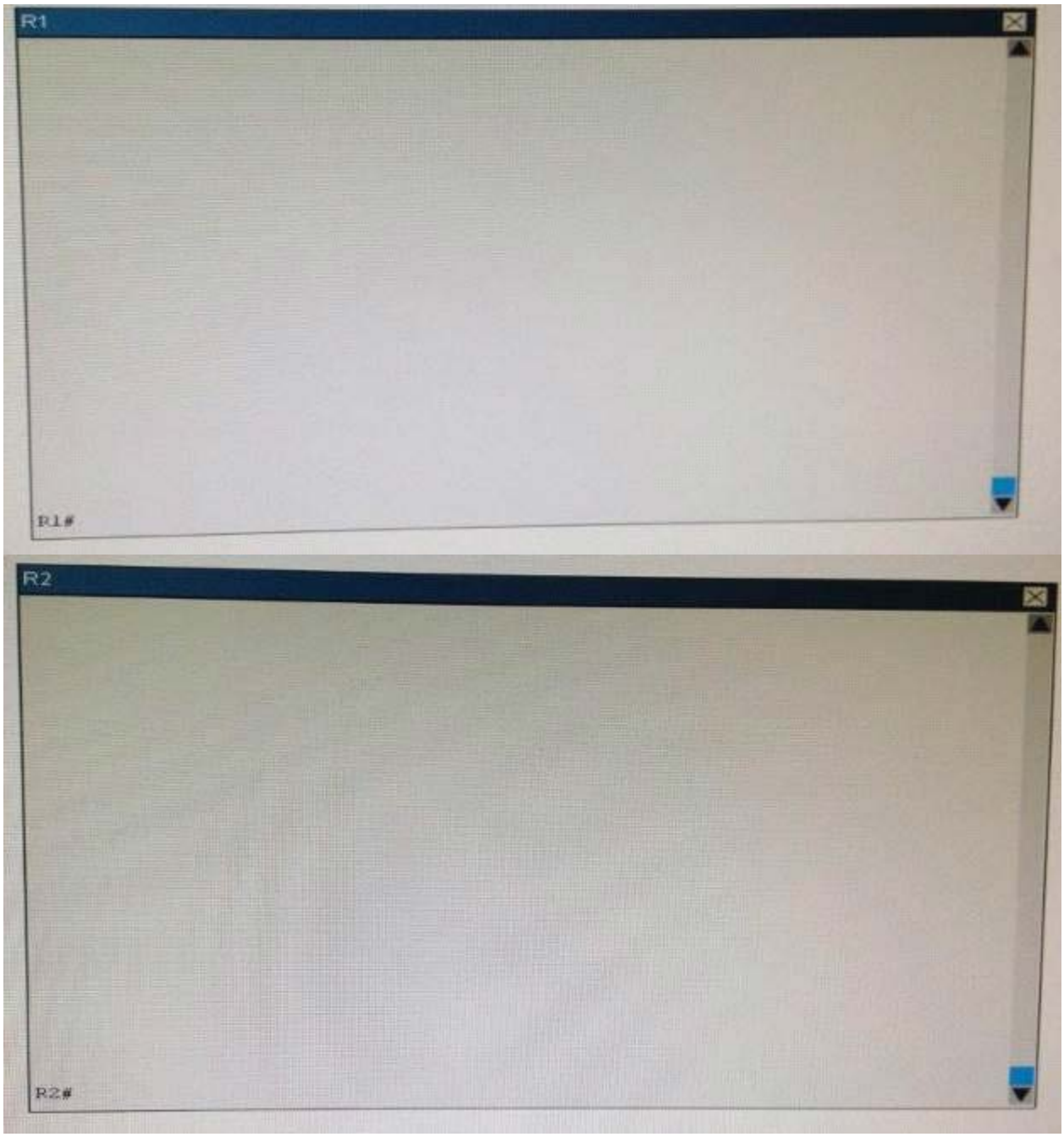
Answer: Select the

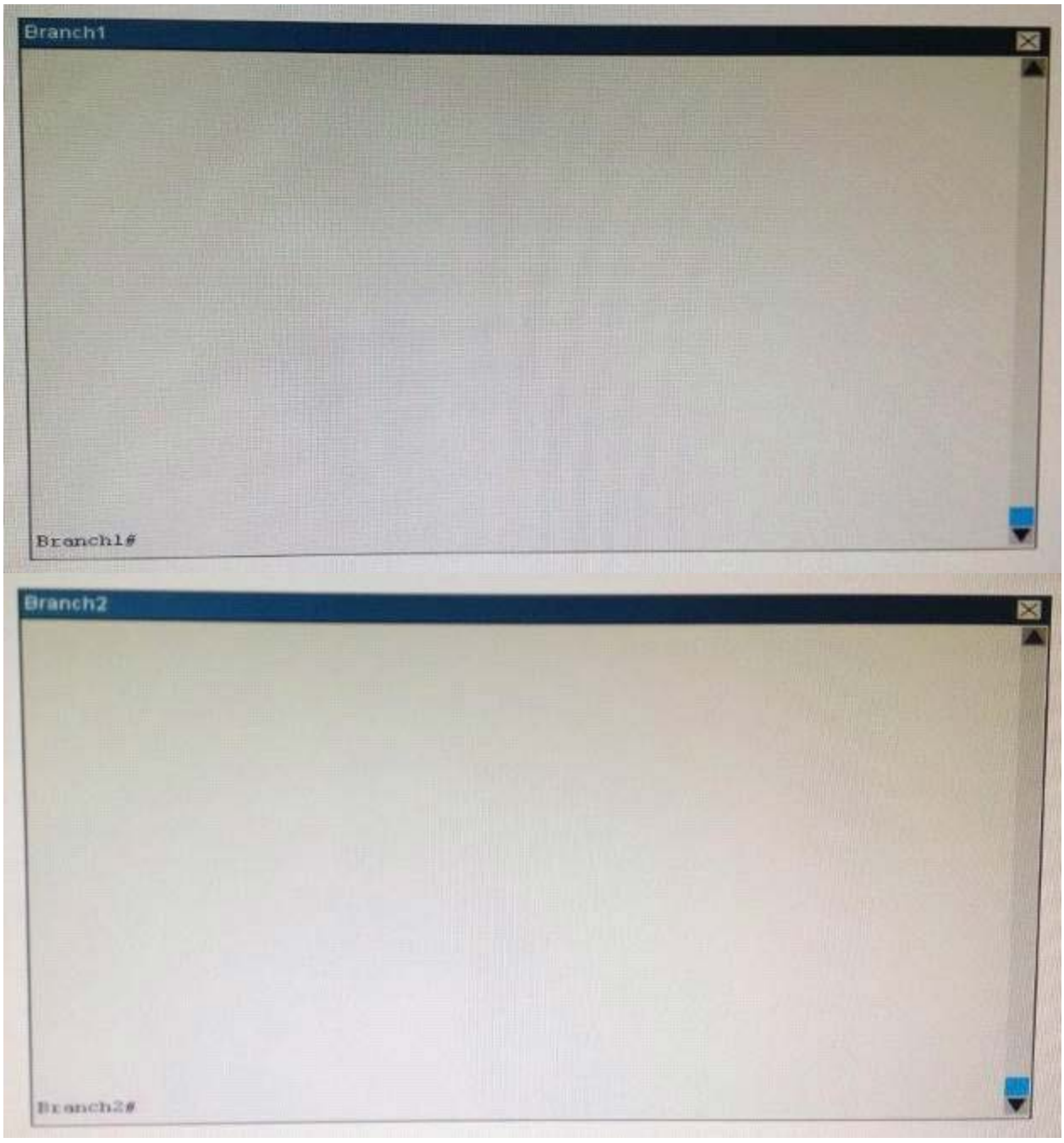
console on Corp1 router

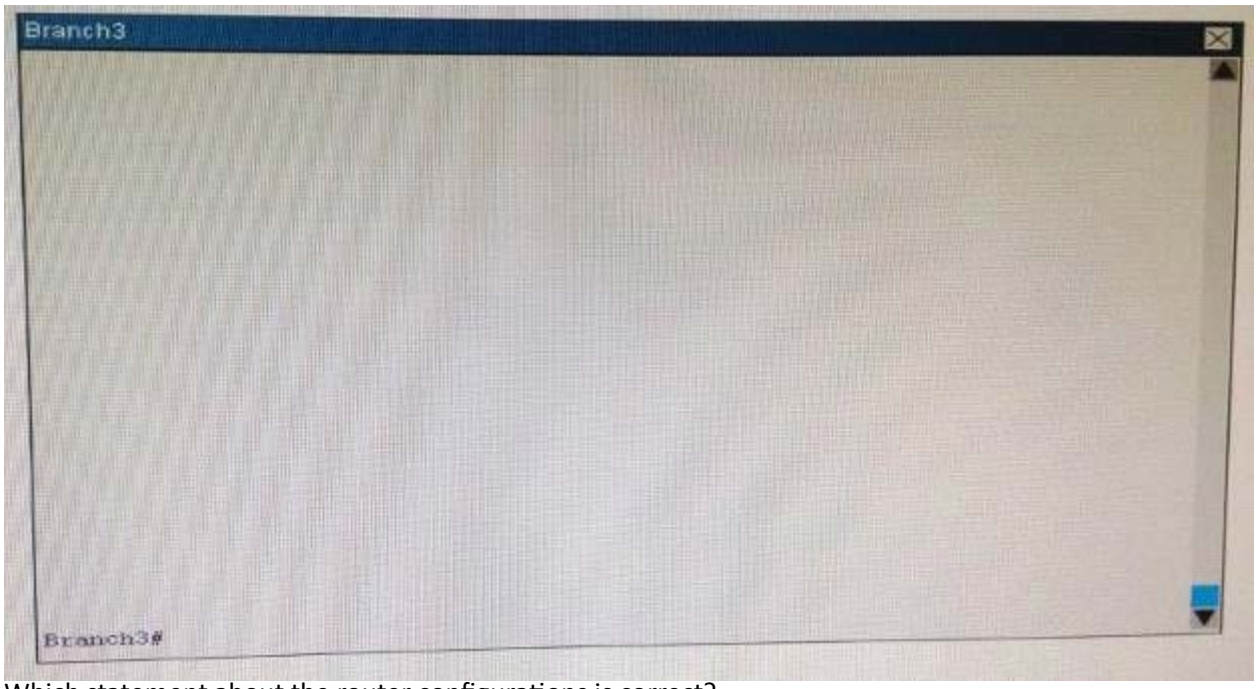
Configuring ACL
Corp1>enable
Corp1#configure terminal
comment: To permit only Host C (192.168.33.3){source addr} to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)
Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
comment: To deny any source to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)
Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80
comment: To permit ip protocol from any source to access any destination because of the implicit deny any any statement at the end of ACL.
Corp1(config)#access-list 100 permit ip any any
Applying the ACL on the Interface
comment: Check show ip interface brief command to identify the interface type and number by checking the IP address configured.
Corp1(config)#interface fa 0/1
If the ip address configured already is incorrect as well as the subnet mask. This should be corrected in order ACL to work
type this commands at interface mode :
no ip address 192.x.x.x 255.x.x.x (removes incorrect configured ipaddress and subnet mask)
Configure Correct IP Address and subnet mask:
ip address 172.22.242.30 255.255.255.240 (range of address specified going to server is given as 172.22.242.17 - 172.22.242.30)
Comment: Place the ACL to check for packets going outside the interface towards the finance web server.
Corp1(config-if)#ip access-group 100 out
Corp1(config-if)#end
Important: To save your running config to startup before exit.
Corp1#copy running-config startup-config
Verifying the Configuration:
Step1: show ip interface brief command identifies the interface on which to apply access list.
Step2: Click on each host A, B, C, & D. Host opens a web browser page, Select address box of the web browser and type the ip address of finance web server (172.22.242.23) to test whether it permits /deny access to the finance web Server.
Step 3: Only Host C (192.168.33.3) has access to the server. If the other host can also access then maybe something went wrong in your configuration. Check whether you configured correctly and in order.
Step 4: If only Host C (192.168.33.3) can access the Finance Web Server you can click on NEXT button to successfully submit the ACL SIM.

Question: 17


Instructions
Enter Cisco IOS commands on the device to verify network operation and answer for multiple choice questions.
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click the device icon to gain access to the console of the router. No console or enable passwords are required.
To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
This task has four multiple-choice questions. Be sure to answer all four questions before clicking the Next button.
Scenario
You are implementing PPP over serial links between R1 router and branch offices. In Phase 1 you must implement and verify PPP and GRE tunnel configurations as mentioned in the topology. In Phase 2 your colleague is expected to do NAT and ISP configurations between R1 and ISP router.
Identify the issues that you encounter during PPP over serial links implementation.
Routers Branch1, Branch2, and Branch3 connect to Router R1 in the main office over serial links.
PPP multilink implementation is recommended between R1 and Branch1 routers.
The GRE tunnel is configured between R2 and Branch2 routers, and traffic between Server farm1 10.10.10.0/24 network and Branch2 LAN 10.10.20.0/24 network, is routed over GRE tunnel using static route.
You have console access on R1, R2, Branch1, Branch2, and Branch3 devices. Use only show commands to troubleshoot the issues.
Topology
Internet
ISP
GRE Tunnel
NAT
Tu0
172.16.10.0/30
192.168.14.0/30
R2
E0/0
R1
Tu0
PPP Multilink
Branch1
192.168.18.0/24
10.10.10.0/24
192.168.12.0/24
L2SW1
PPP
192.168.16.0/30
192.168.15.0/30
PPP
Tu0
S1/0
Branch2
10.10.20.0/24
EIGRP 100
Branch3
192.168.11.0/24
Server farm1
192.168.10.0/24


R1
R1#
R2
R2#


Branch1
Branch1#
Branch2
Branch2#



Which statement about the router configurations is correct?

A. PPP PAP is authentication configured between Branch2 and R1.
B. Tunnel keepalives are not configured for the tunnel0 interface on Branch2 and R2.
C. The Branch2 LAN network 192.168.11 0/24 is not advertised into the EIGRP network.
D. The Branch3 LAW network 192.168.10.0/24 is not advertised into the EIGRP network.
E. PPP CHAP is authentication configured between Branch1 and R1.

Answer: D

THANK YOU FOR DOWNLOADING 200-125 UPDATED EXAM QUESTIONS

Note: Thanks Again For Trying The Demo Of Our 200-125 Exam Product

Visit Our Site to Purchase the Full Set of Actual 200-125 Exam Questions With Answers.

100% Money Back Guarantee

Click The Link Below

https://www.theexamcerts.com/cisco/200-125-pdf-exam-dumps